KRIPTOGRAFI KURVA ELIPTIK ELGAMAL UNTUK PROSES ENKRIPSI-DEKRIPSI CITRA DIGITAL BERWARNA

Nama Mahasiswa	**: Gestihayu Romadhoni F. R**
NRP	**: 1209 100 033**
Jurusan	**: Matematika**
Pembimbing	**: 1. Drs. Daryono B. U, M. Si**
	2. Dian Winda S, S. Si, M. Si

Abstrak

Semakin berkembangnya teknologi dalam beberapa tahun ini, menjadikan semakin banyaknya kemudahan yang diberikan di dalamnya. Salah satunya adalah kemudahan dalam proses pengiriman pesan. Pesan yang dikirim oleh pengirim tidak hanya berupa teks namun pesan juga bisa berupa citra digital. Pesan berupa citra digital yang akan dikirim oleh pengirim harus sampai pada penerima sesuai dengan pesan aslinya. Pada perjalanan proses pengiriman citra digital tersebut sangat rawan terjadi penyadapan dan kebocoran pesan. Proses pengiriman tersebut melalui salah satu jalur pengiriman yang tak aman yakni internet. Dari adanya beberapa permasalahan tersebut perlu adanya suatu proses pengamanan dalam proses pengiriman pesan citra digital tersebut agar pesan yang dikirim atau dibagi dapat diterima dengan utuh. Dalam proses pengamanan tersebut banyak cara untuk mengamankan pesan tersebut, salah satunya yakni dengan kriptografi. Banyak metode dalam kriptografi yang dikembangkan dalam keamanan citra digital saat ini yakni *RSA* dan *ElGamal*, namun kriptografi *RSA* dan

ElGamal dalam mengamankan citra digital tersebut masih belum optimal. Karena pada algoritma *RSA* dan *ElGamal* membutuhkan biaya pengeluaran komputasi yang tinggi dan konsumsi ruang besar, sehingga tidak cocok untuk aplikasi *real-time* dan *bandwidth-limited* (misal transmisi gambar, video streaming dan pengawasan video). Pada tugas akhir ini dibahas mengenai proses enkripsi-dekripsi citra digital berwarna untuk keamanan pesan dengan ECC (*Elliptic Curve Cryptosystem*) atau yang sering dikenal dengan *Elliptic Curve-ElGamal*. Sehingga diharapkan citra digital berwarna tersebut dapat diamankan dari penyadapan maupun kebocoran pesan yang bersifat rahasia. Sehingga pengirim yang ingin mengirimkan pesan berupa citra digital tersebut tidak perlu khawatir untuk berbagi pesan rahasia dengan orang lain.

Kata kunci: Kriptografi, Citra Digital, *Elliptic Curve ElGamal*

ELLIPTIC CURVE ELGAMAL CRYPTOGRAPHY FOR ENCRYPTION-DECRYPTION PROCESS OF COLORED DIGITAL IMAGE

Name	**: Gestihayu Romadhoni F. R**
NRP	**: 1209 100 033**
Department	**: Matematika**
Supervisor	**: 1. Drs. Daryono B. U, M. Si**
	2. Dian Winda S, S. Si, M. Si

Abstract

The continued development of technology in recent years, making so much more convenience provided there in. One is the easy of the process in message delivery. Messages sent by the sender not only text messages but can also in a digital image. Messages are sent by the sender to the recipient must be in accordance with the original message. There is very prone to interception and leak message in the digital image delivery process. The delivery process through one of the transmission line which is unsafe the internet. Because of these issues and therefore needs to be a process of securing the messaging process the digital image to the message to be fully sent or received can be shared. In the process of securing there are many ways to secure the message, one of them is with cryptography. Some developed methods in cryptography in today's digital image security is RSA and ElGamal, but RSA and ElGamal cryptography still have some weakness in securing digital image. Due to the RSA and ElGamal algorithm requires high computational expenses and consumption of a large space, so it is not suitable for real-

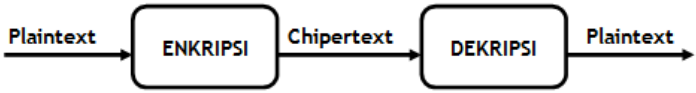
time applications and bandwidth-limited (eg, image transmission, video streaming and video surveillance). In this final project discusses the process of encryption and decryption of colored digital image for message security with ECC (Elliptic Curve Cryptosystem) or sometimes referred to as Elliptic Curve-ElGamal. So the colored digital image can be secured from eavesdropping and leakage of confidential messages can be expected. So the sender who wants to send a message in the form of a digital image does not have to be worry to share private messages with others.

Keywords: Cryptography, Digital Image, Elliptic Curve ElGamal

BAB II
TINJAUAN PUSTAKA

2.1 Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan berita. Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal [4].



Gambar 2.1. Proses enkripsi dan dekripsi

Dapat dilihat pada gambar 2.1 bahwa masukan berupa *plaintext* akan masuk ke dalam blok enkripsi dan keluarannya berupa *chipertext.* Kemudian akan masuk ke dalam blok dekripsi dan keluarannya berupa *plaintext.*

Kriptografi modern menyelesaikan masalah enkripsi dan dekripsi dengan merahasiakan kunci saja tanpa harus merahasiakan algoritmanya. Kunci ini merupakan niai yang sangat spesifik dan bekerja dengan algoritma kriptografi untuk menghasilkan pesan yang terenkripsi secara spesifik pula. Dengan kunci inilah nantinya kita akan dapat melakukan proses enkripsi dan dekripsi. Karena keamanan bergantung pada kerahasiaan kuncinya, maka algoritma yang dibentuk dapat dianalisa dan dipublikasikan .

Berdasarkan jenis kunci yang digunakannya, algoritma kriptografi dikelompokkan menjadi dua bagian, yakni Algoritma Simetris dan Algoritma Asimetris.

2.1.1 Algoritma Simetris

Algoritma Simetris adalah algoritma yang menggunakan kunci yang sama pada proses enkripsi dan dekripsi. Algoritma ini mengharuskan pengirim dan penerima menyetujui satu kunci tertentu. Algoritma yang memakai kunci simetris diantaranya adalah [8] :

1. *Data Encryption Standard* (DES) yakni algoritma yang tergolong jenis blok kode. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsi 64 bit teks-asli menjadi 64 bit teks-kode dengan menggunakan 56 bit *internal key* atau *subkey*. Kunci internal dibangkitkan dari kunci eksternal yang panjangnya 64 bit.
2. *Advance Encryption Standard* (AES) yakni algoritma yang memiliki 3 blok cipher yaitu AES-128, AES-192, AES-256 yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rinjdael. Masing-masing cipher memiliki ukuran 128 bit dengan ukuran kunci masing-masing 128, 192, dan 256 bit.
3. *International Data Encryption Standard* (IDEA) yakni algoritma yang menggunakan konfusi dan difusi. Dari kunci yang mempunyai panjang 128 bit dibangkitkan 52 *subkey*. Algoritma IDEA menggunakan 52 *subkey* dan 16 bit kunci per blok.
4. A5 yakni suatu aliran kode yang digunakan untuk mengamankan percakapan telepon selular GSM. Aliran kodenya terdiri dari 3 buah *Linear Feedback Shift Register* (LSFR) yang dikontrol oleh blok dengan LSFR 19 bit, 22 bit, dan 23 bit. Masing-masing dari LSFR memiliki periode berturut-turut $2^{19}-1, 2^{22}-1$ dan $2^{23}-1$.
5. *One Time Pad* (OTP) yakni algoritma yang berisi deretan kunci yang dibangkitkan secara acak. Setiap kunci hanya digunakan untuk sekali pakai. Pemilihan kunci harus secara acak agar tidak bisa diproduksi ulang dan membuat lawan tidak mudah menerka. Jumlah karakter kunci sama dengan jumlah karakter yang dimiliki pesan.
6. RC2, RC4, RC5, RC6 dan lainnya.

2.1.2 Algoritma Asimetris

Algoritma Asimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Pada algoritma ini, proses enkripsinya menggunakan kunci publik dimana kunci tersebut tidak perlu dijaga kerahasiaanya. Dan untuk proses dekripsinya menggunakan kunci privat dan bersifat rahasia. Algoritma yang memakai kunci asimetris diantaranya adalah [8] :

1. *Digital Signature Algorithm* (DSA) yakni algoritma yang menggunakan kunci umum untuk membuktikan pesan yang diterima sama dengan identitas pengirim data. DSA mempunyai penghitungan yang sulit karena pemisahan algoritma dan berorientasi pada algoritma.ElGamal dan Schnorr.
2. RSA yakni algoritma yang melakukan pemfaktoran bilangan yang sangat besar. Untuk membangkitkan dua kunci, dipilih dua bilangan prima acak yang besar. RSA mengekspresikan teks asli yang dienkripsi menjadi blok-blok yang mana setiap blok memiliki nilai bilangan biner yang diberi symbol “n”, blok teks asli “M” dan blok teks kode “C”. Untuk melakukan enkripsi pesan “M”, pesan dibagi ke dalam blok-blok numerik yang lebih kecil daripada “n” (data biner dengan pangkat terbesar). Jika bilangan prima yang panjangnya 200 digit, dapat ditambah beberapa bit 0 di kiri bilangan untuk menjaga agar pesan tetap kurang dari nilai “n”.
3. Diffie-Hellman (DH) yakni algoritma yang memiliki keamanannya dari kesulitan menghitung logaritma diskrit dalam *finite field,* dibandingkan kemudahan dalam menghitung bentuk eksponensial dalam *finite field* yang sama. Algoritma ini dapat digunakan dalam mendistribusikan kunci public yang dikenal dengan protokol pertukaran kunci
4. *Elliptic Curve Cryptography* (ECC) yakni algoritma yang mendasarkan keamanannya pada permasalahan matematis kurva eliptik. Tidak seperti permasalahan matematis logaritma diskrit dan pemfaktoran bilangan bulat, tidak ada algoritma waktu sub-

eksponensial yang diketahui memecahkan permasalahan matematis algoritma kurva eliptik.

2.2 Citra Digital

Citra digital adalah representasi citra dari fungsi kontinu menjadi nilai-nilai diskrit. Citra digital yang berukuran $M \times N$ lazimnya dinyatakan dengan matriks berukuran M baris dan N kolom, dan masing-masing elemen pada citra digital disebut piksel (*picture element*). Piksel mempunyai dua parameter, yaitu koordinat dan intensitas atau warna. Nilai yang terdapat pada koordinat (x, y) adalah $f(x, y)$, yaitu besar intensitas atau warna dari piksel di titik itu. Oleh sebab itu, sebuah citra digital dapat ditulis dalam bentuk matriks berikut [9].

$$f(x,y) \approx \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,N-1) \\ f(1,0) & f(1,1) & \dots & f(1,N-1) \\ \vdots & \vdots & \dots & \vdots \\ f(M-1,0) & f(M-1,1) & \dots & f(M-1,N-1) \end{bmatrix} \quad (2.1)$$

Berdasarkan gambaran tersebut, secara matematis citra digital dapat dituliskan sebagai fungsi intensitas $f(x, y)$, dimana harga x (baris) dan y (kolom) merupakan koordinat posisi dan $f(x, y)$ adalah nilai fungsi pada setiap titik (x, y) yang menyatakan besar intensitas citra atau warna dari piksel di titik tersebut. Ada banyak cara untuk menyimpan citra digital di dalam memori. Cara penyimpanan menentukan jenis citra digital yang terbentuk. Beberapa jenis citra digital yang sering digunakan adalah citra biner, citra *grayscale*, dan citra warna [9].

2.2.1 Citra Biner (Monokrom)

Citra biner memiliki 2 warna yakni hitam dan putih. Dibutuhkan 1 bit di dalam memori untuk menyimpan kedua warna ini. Intensitas atau warna hitam adalah 0 dan intensitas atau warna putih adalah 1.

2.2.2 Citra *Grayscale* (Skala Keabuan)

Banyaknya warna pada citra *grayscale* tergantung pada jumlah bit yang disediakan di dalam memori untuk menampung kebutuhan warna ini. Citra 2 bit mewakili 4 warna, citra 3 bit mewakili 8 warna, citra 4 bit mewakili 16 warna dst.

2.2.3 Citra Warna *(True Color)*

Setiap piksel pada citra warna mewakili warna yang merupakan kombinasi dari tiga warna dasar (RGB = *Red Green Blue*). Setiap warna dasar menggunakan penyimpanan 8 bit = 1 *byte,* yang berarti setiap warna mempunyai gradasi sebanyak 255 warna. Berarti setiap piksel mempunyai kombinasi warna sebanyak $2^8 \cdot 2^8 \cdot 2^8 = 2^{24} = 16$ juta warna lebih. Itulah sebabnya format ini dinamakan *true color* karena mempunyai jumlah warna yang cukup besar sehingga bisa dikatakan hampir mencakup semua warna di alam.

2.3 Polinomial

Suatu grup adalah suatu himpunan $G \neq \emptyset$ dengan operasi biner $* : G \times G \to G$ yang mana untuk setiap (a, b) di $G \times G$, dengan $a * b \in G$, sedemikian hingga sifat-sifat berikut dipenuhi [5]:

1. $(a * b) * c = a * (b * c)$ untuk semua $a, b, c \in G$.
2. Ada $e \in G$, sedemikian hingga $e * g = g = g * e$ untuk semua $g \in G$; e disebut unsur identitas pada G.
3. Untuk setiap $g \in G$ ada $g^{-1} \in G$ yang memenuhi $g * g^{-1} = e = g^{-1} * g$

Jika $a * b = b * a$ untuk semua $a, b \in G$, maka grup G dinamakan grup *abelian/komutatif*

Notasi $\langle G, * \rangle$ menyatakan sebuah grup dengan operasi biner $*$. Notasi $\langle G, + \rangle$ disebut dengan grup penjumlahan dan $\langle G, \cdot \rangle$ disebut dengan grup perkalian. Pada grup penjumlahan, elemen netral disimbolkan dengan 0 dan invers dari a dinyatakan sebagai $-a$. Sedangkan grup perkalian elemen netral disimbolkan dengan 1 dan invers dari a dinyatakan sebagai a^{-1} [5].

Sebagai contoh integer modulo n, ditulis sebagai $Z_n = \{0, 1, 2, \dots, n-1\}$ merupakan bentuk sebuah grup pada operasi penjumlahan modulo n. Jika p adalah bilangan prima, maka elemen-elemen bukan nol Z_p dapat ditulis sebagai $Z^*{}_p = \{1, 2, \dots, p-1\}$, merupakan bentuk sebuah grup pada operasi perkalian modulo p. Nilai elemen $g \in G$ adalah bilangan integer positif terkecil n sehingga $g^n = 1$. Contoh untuk $Z^*{}_{11}$ dengan elemen $g = 3$ memiliki 5 buah nilai, yaitu :

$$3^1 \equiv 3 \pmod{11}$$
$$3^2 \equiv 9 \pmod{11}$$
$$3^3 \equiv 5 \pmod{11}$$
$$3^4 \equiv 4 \pmod{11}$$
$$3^5 \equiv 1 \pmod{11}$$

Suatu lapangan *(Field)* adalah suatu himpunan $K \neq \emptyset$ bersama-sama dengan dua operasi tambah $(+)$ dan kali $(-)$ sehingga untuk semua $a, b, c \in K$ memenuhi [12] :

- $a + b \in K$ (tertutup)
- $a + b = b + a$ (komutatif)
- $(a + b) + c = a + (b + c)$ (assosiatif)
- Ada $0 \in K$ sehingga $a + 0 = 0 + a = a$ (elemen netral)
- Untuk setiap $a \in K$ ada suatu $-a \in K$ sehingga $a + (-a) = -a + a = 0$ (invers)
- $a \cdot b \in K$ (tertutup)
- $a \cdot b = b \cdot a$ (komutatif)
- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (assosiatif)
- Ada $1 \in K$ sehingga $a \cdot 1 = 1 \cdot a = a$ (elemen identitas)
- Bila $a \neq 0$ dan $a \in K$, maka ada $a^{-1} \in K$ sehingga $a \cdot a^{-1} = a^{-1} \cdot a = 1$ (invers)
- $a \cdot (b + c) = a \cdot b + a \cdot c$ dan $(a + b) \cdot c = a \cdot c + b \cdot c$ (distributif)

Dari pengertian di atas suatu himpunan $K \neq \emptyset$ dikatakan lapangan jika

i. $(K, +)$ grup abel

ii. $(K - \{0\}, \cdot)$ grup abel

iii. $(K, +, \cdot)$ bersifat distributif yaitu $a \cdot (b + c) = a \cdot b + a \cdot c$ dan $(a + b) \cdot c = a \cdot c + b \cdot c$

Misalkan p adalah bilangan prima, bilangan bulat modulo p terdiri dari $\{0, 1, 2, \ldots, p-1\}$ dengan penjumlahan dan perkalian oleh modulo p, adalah lapangan berhingga.

Sebuah polinomial atas lapangan K dinyatakan dalam bentuk [14]:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,\ a_i \in K \qquad (2.2)$$

Misalkan,

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n,\ a_i \in K \qquad (2.3)$$

$$g(x) = b_0 + b_1 x + \cdots + b_m x^m,\ a_j \in K \qquad (2.4)$$

Penjumlahan $f(x)$ dan $g(x)$ dinyatakan sebagai:

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_1 + b_1)x^2 + \cdots \qquad (2.5)$$

Perkalian $f(x)$ dan $g(x)$ dinyatakan sebagai:

$$\begin{aligned} f(x) \cdot g(x) &= (a_0 + a_1 x + \cdots + a_n x^n)(b_0 + b_1 x + \cdots + b_m x^m) \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots \\ &= c_0 + c_1 x + c_2 x^2 + \cdots + c_{n+m} x^{n+m} \qquad (2.6) \end{aligned}$$

dimana $c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0$

2.4 ECC (*Elliptic Curve Cryptosystem*)

Elliptic Curve Cryptosystem (ECC) diperkenalkan tahun 1985 oleh Neal Koblity dan Victor Miller dari Universitas Washington. Kurva eliptik mempunyai masalah logaritma yang terpisah sehingga sulit untuk dipecahkan. Pada Juni 2000 kunci enkripsi ECC yang memakai 108 bit (yang setara dengan kunci enkripsi RSA 600 bit), berhasil dipecahkan menggunakan 9500 komputer yang berjalan paralel selama 4 bulan yang dihubungkan dengan internet.

Kriptografi kurva eliptik termasuk sistem kriptografi kunci publik yang mendasarkan keamanannya pada permasalahan matematis kurva eliptik. Tidak seperti permasalahan matematis logaritmis diskrit (*Discrete Logarithm Problem,* DLP) dan pemfaktoran bilangan bulat (*Integer Factorization Problem,* IFP), tidak ada algoritma waktu sub-eksponensial yang diketahui untuk memecahkan permasalahan matematis algoritma diskrit kurva eliptik (*Elliptic Curve Discrete Logarithm Problem,* ECDLP). Oleh karena alasan tersebut algoritma kurva eliptik mempunyai keuntungan bila dibanding algoritma kriptografi kunci publik lainnya, yaitu dalam hal ukuran kunci yang lebih pendek tetapi memiliki tingkat keamanan yang sama [8].

2.5 Kurva Eliptik

Kurva eliptik yang digunakan dalam kriptografi didefinisikan dengan menggunakan dua tipe daerah terbatas yakni daerah karakteristik ganjil (F_p dimana $p > 3$ adalah bilangan prima yang besar) dan karakteristik dua ($F2^m$). Karena perbedaan itu menjadi tidak begitu penting, kedua daerah terbatas tersebut dapat ditunjukkan sebagai F_q , dimana $q = p$ atau $q = 2^m$. Elemen dari F_p adalah integer $(0 \leq x < p)$ dimana elemen tersebut dapat dikombinasikan menggunakan modul aritmatik [8].

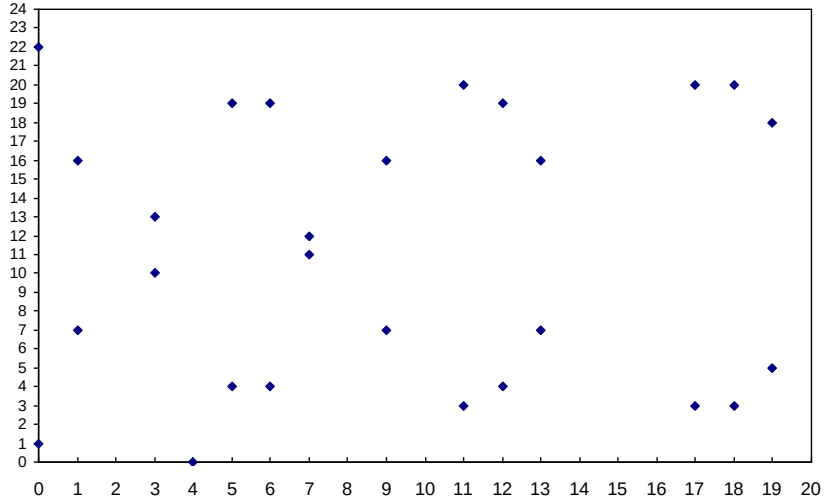
Pada bagian ini akan dibahas teknik dasar kurva eliptik dalam bidang terbatas F_p dimana p adalah bilangan prima lebih besar dari 3. Selanjutnya kurva eliptik secara umum didefinisikan sebagai *field* berhingga (*finite field*). Sebuah kurva eliptik E pada bidang terbatas F_p didefinisikan dalam persamaan :

$$y^2 = x^3 + ax + b(mod\ p) \qquad (2.7)$$

dimana $a, b \in F_p$ dan $4a^3 + 27b^2 \neq 0$ dan sebuah titik **O** yang disebut titik tak hingga (*infinity)*. Titik tak hingga adalah identitas. Himpunan $E(F_p)$ adalah semua titik (x, y) untuk $x, y \in F_p$ yang memenuhi persamaan (2.7) pada titik **O.**

Untuk menjelaskan uraian di atas, berikut ini diberikan contoh pencarian himpunan $E(F_p)$. Diberikan persamaan kurva eliptik E: $y^2 = x^3 + x + 1$ dengan $p = 23$, yaitu grup F_{23} (a = b = 1). Maka untuk nilai $4a^3 + 27b^2 = 4 + 27 \neq 0$, sehingga E ada dalam kurva eliptik. Titik-titik dalam $E(F_{23})$ adalah :

(0,1)	(6,4)	(12,19)
(0,22)	(6,19)	(13,7)
(1,7)	(7,11)	(13,16)
(1,16)	(7,12)	(17,3)
(3,10)	(9,7)	(17,20)
(3,13)	(9,16)	(18,3)
(4,0)	(11,3)	(18,20)
(5,4)	(11,20)	(19,5)
(5,19)	(12,4)	(19,18)



Gambar 2.2. Sebaran titik – titik pada kurva eliptik $E(F_{23})$ untuk $E: y^2 = x^3 + x + 1$

2.5.1 Kurva Eliptik pada Himpunan F_p

Pada bidang terbatas F_p perhitungan dilakukan dengan menggunakan aturan-aturan aritmatika modular. Persamaan kurva eliptik pada F_p dapat dituliskan sebagai berikut :

$$y^2 \bmod p = (x^3 + ax + b) \bmod p \quad a, b \in F_p \qquad (2.8)$$

dengan p adalah bilangan prima ganjil dan $p >$.

F_p (a, b) adalah himpunan yang terdiri atas titik-titik (x, y) yang memenuhi persamaan (2.7) ditambah dengan titik **O** yang disebut titik *infinity*. Kurva eliptik pada bidang terbatas F_p merupakan grup abelian, apabila sisi kanan persamaan (2.7) tidak memiliki faktor yang berulang yaitu apabila koefisien-koefisiennya memenuhi persamaan $a^3 + \quad b^2 (mod\ p) \neq \quad (mod\ p)$.

Operasi yang berlaku dalam bidang terbatas F_p adalah [8]:

1. Penjumlahan (*addition*), jika $a, b \in F_p$, maka $a + b = r$, dimana r adalah sisa pembagian $a + b$ dengan bilangan

prima p, $\leq r \leq p -$. Penjumlahan seperti ini disebut penjumlahan modulo p (mod p).

2. Perkalian (*multiplication*), jika $a, b \in F_p$, maka $a.b = s$, dimana s adalah sisa pembagian $a.b$ dengan bilangan prima p, $\leq s \leq p -$. Perkalian seperti ini perkalian modulo p (mod p).

Penjumlahan dua buah titik $P(x_1, y_1)$ dan $Q(x_2, y_2)$ adalah (x_3, y_3) dengan syarat bahwa P ≠ **O** dan Q ≠ P. Secara aljabar, (x_3, y_3) diperoleh dengan rumus berikut [7]:

$$\lambda = \left(\frac{y_2 - y_1}{x_2 - x_1}\right) \qquad \text{Jika P} \neq \text{Q} \qquad (2.9)$$

$$\lambda = \left(\frac{3{x_1}^2 + a}{2y_1}\right) \qquad \text{Jika P} = \text{Q} \qquad (2.10)$$

$$x_3 = \lambda \ - x_1 - x_2 \qquad (2.11)$$

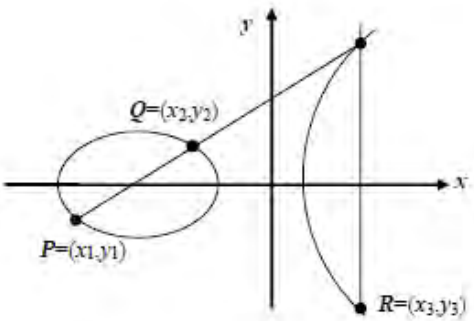
$$y_3 = -y_1 + \lambda\,(x_1 - x_3) \qquad (2.12)$$

Operasi penjumlahan pada kurva eliptik atas F_p didefinisikan sebagai berikut [8] :

a. **O** adalah identitas penjumlahan, sehingga P + **O** = **O** + P = P untuk setiap P ∈ $E(F_p)$.
b. Jika P = (x, y) maka P + $(x, -y) = \mathbf{O}$. Titik $(x, -y)$ adalah negatif P, dilambangkan dengan –P.
c. Misalkan P = $(x_1, y_1) \in E(F_p)$ dan titik Q = $(x_2, y_2) \in E(F_p)$ dimana P ≠ **O**, Q ≠ **O**, dan Q ≠ ± P. Maka P + Q = (x_3, y_3) dimana :

$$x_3 = \left[\left(\frac{y_2 - y_1}{x_2 - x_1}\right) \ - x_1 - x_2\right] \bmod \text{p} \qquad (2.13)$$

$$y_3 = \left[\left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1\right] \bmod \text{p} \qquad (2.14)$$

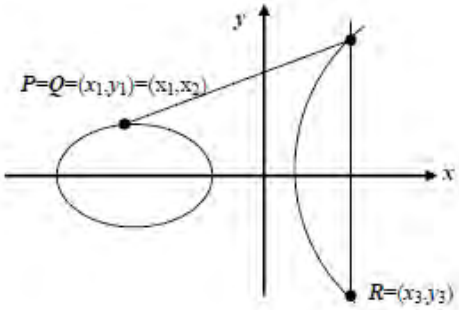


Gambar 2.3. Gambaran secara geometri penjumlahan dua titik berbeda [7]

d. Misalkan P = $(x_1, y_1) \in E(F_p)$, maka P + P = 2P = (x_3, y_3) dimana :

$$x_3 = \left[\left(\frac{3{x_1}^2 + a}{2y_1}\right)^2 - 2x_1\right] \bmod p \qquad (2.15)$$

$$y_3 = \left[\left(\frac{3x_1 + a}{2y_1}\right)(x_1 - x_3) - y_1\right] \bmod p \qquad (2.16)$$



Gambar 2.4. Gambaran secara geometri penjumlahan dua titik sama [7]

2.6 Domain Parameter Kurva Eliptik

Pada subbab ini dibahas tentang domain parameter-parameter kurva eliptik atas F_p. Sebelum mengimplementasikan kriptografi kurva eliptik, dipersiapkan parameter yang dibutuhkan oleh sistem kriptografi tersebut. Sehingga seluruh pengguna sistem dapat mengetahui beberapa parameter yang akan digunakan bersama. Parameter ini bersifat umum dan boleh diketahui oleh setiap pengguna sistem tersebut.

Pembuatan domain parameter tersebut tidak dilakukan oleh masing-masing pengirim atau penerima karena akan melibatkan perhitungan jumlah titik pada kurva yang akan memakan waktu yang lama dan sulit untuk diterapkan. Sehingga dipilih standar domain parameter kurva eliptik yakni SEC 2 (*Standards Efficient Cryptography : Recommended Elliptic Curve Domain Parameters*). Domain parameter kurva eliptik atas F_p yang sesuai standar SEC 2 didefinisikan sebagai berikut [1]:

$$T = (p, a, b, G, n, h) \qquad (2.17)$$

Dimana

p : bilangan prima
a, b : koefisien persamaan kurva eliptik
G : titik dasar yaitu elemen pembangun grup kurva eliptik
n : order dari G yaitu bilangan bulat positif terkecil $\ni n.\ G =$O
h : kofaktor, $h = \#E/n$, $\#E$ adalah jumlah titik dalam grup eliptik $E_p(a, b)$

Kekuatan kriptografi kurva eliptik bergantung dari pemilihan parameter domain yang digunakan. Pemilihan parameter ini dilakukan sehingga dapat terhindar dari serangan terhadap kekuatan algoritma kriptografi kurva eliptik.

BAB III
METODOLOGI PENELITIAN

Pada bab ini dijelaskan mengenai tahapan-tahapan dalam menyelesaikan permasalahan yang ada di dalam tugas akhir ini.

3.1 Studi Literatur

Dalam tahap ini dilakukan proses analisa kurva eliptik, analisa algoritma ECC *(Elliptic Curve Cryptosystem)* atau EC-ElGamal, baca Citra dari bentuk JPG ke dalam file .txt. Studi literatur ini diperoleh dari berbagai modul, jurnal ilmiah, buku teks dan laporan tugas akhir yang berkaitan dengan sistem maupun beberapa artikel yang ada di internet.

3.2 Perancangan Sistem EC-ElGamal dan Implementasi *Interface*

Pada tahap perancangan sistem ini, citra asli berwarna (RGB) dilakukan proses enkripsi dan dekripsi dengan algoritma EC-ElGamal. Sebelum melakukan proses enkripsi dan dekripsi citra, terlebih dahulu dengan membuat titik-titik pada kurva eliptik dan mencari titik ketiga. Titik ketiga ini yang nantinya akan digunakan sebagai kunci publik dalam proses enkripsi dan dekripsi citra.

Akan tetapi pada pembuatan program pada tugas akhir ini, tidak menggunakan titik ketiga sebagai kunci publik, namun menggunakan parameter yang telah diberikan oleh kriptografi. Pembuatan parameter domain tersebut tidak dilakukan oleh masing-masing pengirim atau penerima karena akan melibatkan perhitungan jumlah titik pada kurva yang akan memakan waktu yang lama dan sulit untuk diterapkan. Sehingga dipilih standar parameter domain kurva eliptik yakni SEC 2 (*Standards Efficient Cryptography : Recommended Elliptic Curve Domain Parameters*).

Setelah dilakukan pemilihan terhadap parameter, selanjutnya dilakukan proses pembacaan piksel citra ke dalam file .txt yang nantinya akan menjadi *plaintext* pada proses enkripsi citra. Setelah dilakukan proses enkripsi citra, maka file citra asli yang telah dienkrip berupa *chipertext* dikembalikan ke bentuk semula dengan proses dekripsi dan ditampilkan dalam *interface* dan kembali menjadi citra asli.

Dalam tahap ini dilakukan perancangan dan implementasi *interface* dengan menggunakan bahasa Java di NetBeans IDE 6.9.1.

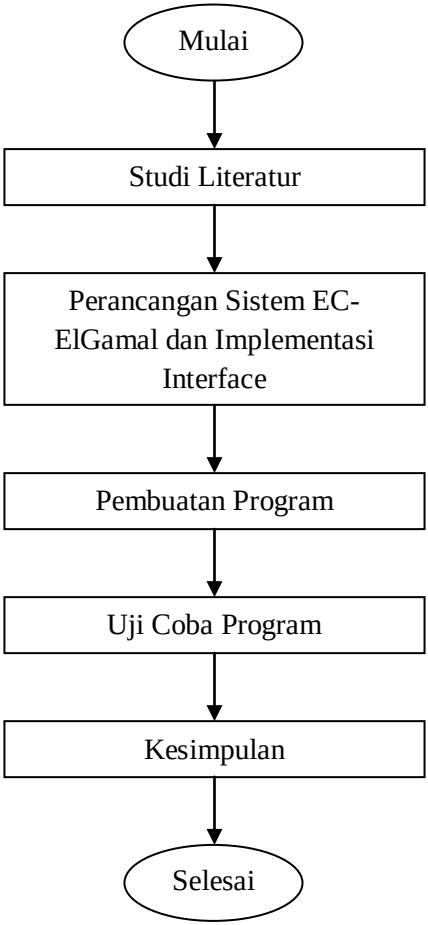
3.3 Pembuatan Program

Pada tahap ini akan dilakukan proses pembuatan program dengan berdasarkan perancangan sistem enkripsi dan dekripsi citra yang telah dibuat menggunakan NetBeans 6.9.1 dengan bahasan pemrograman Java.

3.4 Uji Coba Program

Pada tahap ini akan dilakukan uji coba terhadap program yang telah dibuat dengan memberikan input yang berbeda namun masih dalam batasan yang sudah ditentukan dalam tugas akhir ini.

Diagram alir dari metode penelitian diatas dapat digambarkan sebagai berikut :



Gambar 3.1. Diagram alir metode penelitian

BAB IV
PERANCANGAN DAN IMPLEMENTASI SISTEM

Pada bab ini dibahas mengenai perancangan dan implementasi dari sistem EC-ElGamal. Perancangan sistem meliputi perancangan kurva eliptik di bidang F_p, domain parameter, pembangkitan kunci publik dan kunci privat, perancangan sistem enkripsi dan dekripsi citra. Implementasi sistem meliputi pembuatan program secara keseluruhan dengan menggunakan bahasa java Netbeans IDE.

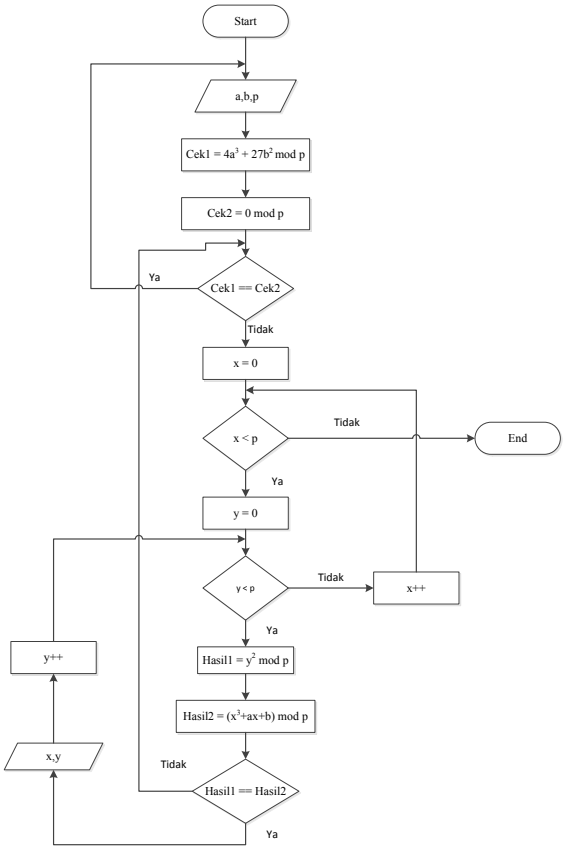
4.1 Perancangan Kurva Eliptik di Bidang F_p

Sistem kriptografi tidak menggunakan kurva eliptik pada bilangan real namun menggunakan medan terbatas misalnya medan modular bilangan prima F_p. Pada bidang terbatas F_p perhitungan dilakukan dengan menggunakan aturan-aturan aritmatika modular. Persamaan kurva eliptik pada F_p dapat dituliskan seperti persamaan (2.7) dengan p adalah bilangan prima ganjil dan $p > 3$. F_p (a, b) adalah himpunan yang terdiri atas titik-titik (x, y) yang memenuhi persamaan (2.8) ditambah dengan titik **O** yang disebut titik *infinity*. Kurva eliptik pada bidang terbatas F_p merupakan grup abelian, apabila sisi kanan persamaan (2.8) tidak memiliki faktor yang berulang yaitu apabila koefisien – koefisiennya memenuhi persamaan $4a^3 + 27b^2 (\text{mod } p) \neq 0 \ (\text{mod } p)$.

4.1.1 Pembuatan Titik (x, y)

Pada gambar 4.1 dijelaskan bahwa nilai a, b dan p berupa bilangan real, untuk nilai a dan $b \in F_p$. Kemudian nilai a, b dan p diproses sesuai dengan persamaan $a^3 + b^2 (mod\ p) \neq (mod\ p)$, jika tidak memenuhi persamaan tersebut maka harus kembali ke awal untuk memasukkan nilai a, b dan p. Jika memenuhi persamaan tersebut maka proses akan berlanjut untuk menemukan titik (x, y) yakni dengan syarat $x < p$, jika tidak memenuhi maka berhenti dari proses, dan jika memenuhi maka

berlanjut untuk syarat $y < p$. Jika syarat tersebut tidak terpenuhi, maka berlanjut untuk syarat $x{+}{+}$ dan kembali ke awal syarat $x < p$. Jika syarat tersebut terpenuhi maka akan menuju ke proses selanjutnya yakni hasil 1 = $y^2 \ mod \ p$ dan hasil 2 = $(x^3 + ax + b) \ mod \ p$. Jika hasil 1 ≠ hasil 2 maka proses akan kembali pada pengecekan persamaan $a^3 + \ b^2 (mod \ p) \neq \ (mod \ p)$, jika hasil 1 = hasil 2 maka akan ditemukan titik (x, y) dan proses tersebut berulang (y ++) terus sampai syarat $x < p$ tidak terpenuhi.



Gambar 4.1. Flowchart pembuatan titik (x, y)

Contoh perhitungan secara aljabar untuk pembuatan titik kurva eliptik, diberikan persamaan kurva eliptik $E: y^2 = x^3 + x + 5$ dengan $p = 17$, yaitu grup F_{17} (a = 1, b = 5). Maka untuk nilai $4a^3 + 27b^2 = 4(1) + 27(25) \neq 0$, sehingga E ada dalam kurva eliptik.

- Untuk dapat membuat titik kurva (x, y), pertama tentukan elemen dari kurva eliptik $E_{17}(1,5)$ atas F_p.

$$F_p = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\}$$

- Sebelum menentukan daerah elemen kurva eliptik $E_{17}(1,5)$, terlebih dahulu mencari QR_{17} (Quadratic Residue Module) [11].

Tabel 4.1. Hasil QR_{17}(Quadratic Residue Module)

F_p	$y^2 (mod\ 17)$	QR_{17}
0	$0^2 (mod\ 17)$	0
1	$1^2 (mod\ 17)$	1
2	$2^2 (mod\ 17)$	4
3	$3^2 (mod\ 17)$	9
4	$4^2 (mod\ 17)$	16
5	$5^2 (mod\ 17)$	8
6	$6^2 (mod\ 17)$	2
7	$7^2 (mod\ 17)$	15
8	$8^2 (mod\ 17)$	13
9	$9^2 (mod\ 17)$	13
10	$10^2 (mod\ 17)$	15
11	$11^2 (mod\ 17)$	2
12	$12^2 (mod\ 17)$	8
13	$13^2 (mod\ 17)$	16
14	$14^2 (mod\ 17)$	9
15	$15^2 (mod\ 17)$	4
16	$16^2 (mod\ 17)$	1

Jadi, didapat $QR_{17} = \{0,1,2,4,8,9,13,15,16\}$

- Menentukan elemen grup kurva eliptik $E_{17}(1,5)$ yang merupakan himpunan penyelesaian dari $y^2 = x^3 + x + 5\ (mod\ 17)$ untuk $x \in F_{17}$ dan $y^2 = QR_{17}$

Tabel 4.2. Elemen grup kurva eliptik

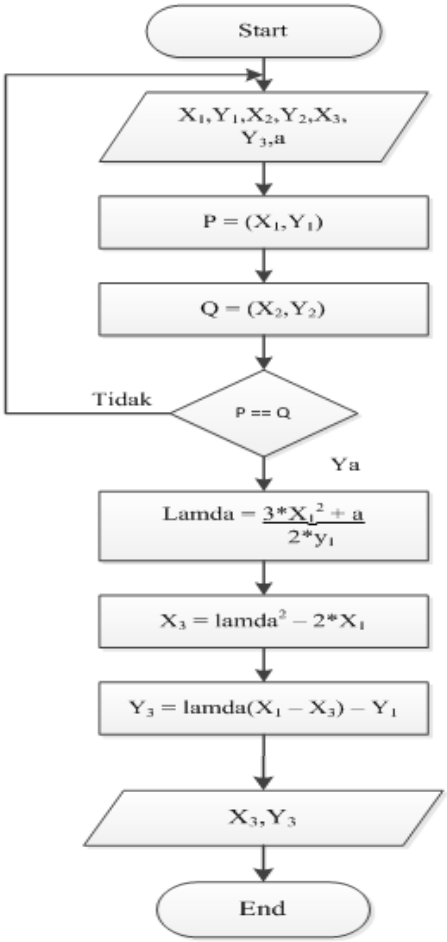
$x \in F_{17}$	$y^2 = x^3 + x + 5 \ (mod\ 17)$	$y^2 \in QR_{17}$	$(x, y) \in E_{17}(1, 5)$
$x = 0$	$y^2 = 0^3 + 0 + 5 \ (mod\ 17)$ $= 5$	$5 \notin QR_{17}$	–
$x = 1$	$y^2 = 1^3 + 1 + 5 \ (mod\ 17)$ $= 7$	$7 \notin QR_{17}$	–
$x = 2$	$y^2 = 2^3 + 2 + 5 \ (mod\ 17)$ $= 15$	$15 \in QR_{17}$	(2,7) dan (2,10)
$x = 3$	$y^2 = 3^3 + 3 + 5 \ (mod\ 17)$ $= 35 (mod\ 17)$ $= 1$	$1 \in QR_{17}$	(3,1) dan (3,16)
$x = 4$	$y^2 = 4^3 + 4 + 5 \ (mod\ 17)$ $= 73 (mod\ 17)$ $= 5$	$5 \notin QR_{17}$	–
$x = 5$	$y^2 = 5^3 + 5 + 5 \ (mod\ 17)$ $= 135 (mod\ 17)$ $= 16$	$16 \in QR_{17}$	(5,4) dan (5,13)
$x = 6$	$y^2 = 6^3 + 6 + 5 \ (mod\ 17)$ $= 227 (mod\ 17)$ $= 6$	$6 \notin QR_{17}$	–
$x = 7$	$y^2 = 7^3 + 7 + 5 \ (mod\ 17)$ $= 355 (mod\ 17)$ $= 15$	$15 \in QR_{17}$	(7,7) dan (7,10)
$x = 8$	$y^2 = 8^3 + 8 + 5 \ (mod\ 17)$ $= 525 (mod\ 17)$ $= 15$	$15 \in QR_{17}$	(8,7) dan (8,10)
$x = 9$	$y^2 = 9^3 + 9 + 5 \ (mod\ 17)$ $= 743 (mod\ 17)$ $= 12$	$12 \notin QR_{17}$	–
$x = 10$	$y^2 = 10^3 + 10 + 5 \ (mod\ 17)$ $= 1015 (mod\ 17)$ $= 12$	$12 \notin QR_{17}$	–
$x = 11$	$y^2 = 11^3 + 11 + 5 \ (mod\ 17)$ $= 1347 (mod\ 17)$ $= 4$	$4 \in QR_{17}$	(11,2) dan (11,15)

$x = 12$	$y^2 = 12^3 + 12 + 5\ (mod\ 17)$ $= 1745(mod\ 17)$ $= 11$	$11 \notin QR_{17}$	–
$x = 13$	$y^2 = 13^3 + 13 + 5\ (mod\ 17)$ $= 2215(mod\ 17)$ $= 5$	$5 \notin QR_{17}$	–
$x = 14$	$y^2 = 14^3 + 14 + 5\ (mod\ 17)$ $= 2763(mod\ 17)$ $= 9$	$9 \in QR_{17}$	(14,3) dan (14,14)
$x = 15$	$y^2 = 15^3 + 15 + 5\ (mod\ 17)$ $= 3395(mod\ 17)$ $= 12$	$12 \notin QR_{17}$	–
$x = 16$	$y^2 = 16^3 + 16 + 5\ (mod\ 17)$ $= 4117(mod\ 17)$ $= 3$	$3 \notin QR_{17}$	–

Jadi, titik-titik dalam kurva eliptik adalah
$E_{17}(1,5)$

4.1.2 Pembuatan Titik Ketiga (x_3, y_3)

Pada gambar 4.2 menjelaskan proses pembuatan titik ketiga di bidang terbatas f_p dengan penjumlahan dua titik yang sama. Pada proses pembuatan titik ketiga ini terdapat dua titik yang sama yakni $P = (x_1, y_1)$ dan $Q = (x_2, y_2)$, untuk nilai $x_1, y_1, x_2, y_2, x_3, y_3 \in E(F_p)$. Syarat pertama untuk proses ini adalah P = Q, jika syarat tersebut tidak terpenuhi maka kembali ke awal untuk x_1, y_1, x_2, y_2, jika syarat terpenuhi maka ke proses selanjutnya yakni melakukan penghitungan menggunakan rumus lamda pada persamaan (2.10). Setelah nilai lamda ditemukan, kemudian x_3 dapat dihitung dengan menggunakan persamaan (2.15). Selanjutnya y_3 dapat dihitung dengan menggunakan persamaan (2.16). Titik ketiga x_3, y_3 telah ditemukan dari proses diatas dan diagram alir proses pembuatan titik ketiga dengan penjumlahan dua titik yang sama dapat dilihat pada gambar 4.2.



Gambar 4.2. Flowchart pembuatan titik ketiga dengan penjumlahan dua titik sama

Contoh perhitungan secara aljabar untuk pembuatan titik ketiga dengan titik awal sama, untuk persamaan kurva eliptik $E: y^2 = x^3 + x + 5$ dengan $a = 1,\ b = 5,\ p = 17$ didapatkan titik kurva eliptik

$$(x,y) = \begin{Bmatrix} (2,7),(2,10),(3,1),(3,16),(5,4),(5,13),(7,7),(7,10), \\ (8,7),(8,10),(11,2),(11,15),(14,3),(14,14) \end{Bmatrix}$$

Untuk $P = (x_1, y_1)$ dan $Q = (x_2, y_2)$ maka $P = Q = P + P = 2P = (x_3, y_3)$ dimana :

$$x_3 = \left[\left(\frac{3x_1 + a}{2y_1}\right) - 2x_1\right] mod\ p$$

$$y_3 = \left[\left(\frac{3x_1 + a}{2y_1}\right)(x_1 - x_3) - y_1\right] mod\ p$$

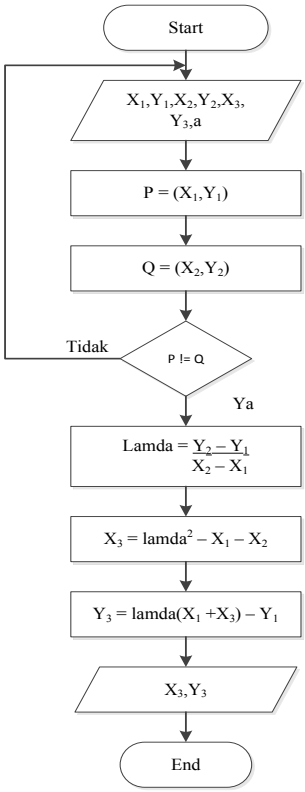
Ambil $P = (3,1)$ maka $2P = P + P = (x_3, y_3)$, perhitungannya seperti di bawah ini:

$$x_3 = \left[\left(\frac{3x_1 + a}{2y_1}\right) - 2x_1\right] mod\ p$$
$$= \left[\left(\frac{3(3)^2+1}{2(1)}\right)^2 - 2(3)\right] (mod\ 17)$$
$$= \left[\left(\frac{28}{2}\right)^2 - 6\right] (mod\ 17)$$
$$= [14^2 - 6] (mod\ 17)$$
$$= 190 (mod\ 17)$$
$$= 3$$
$$y_3 = \left[\left(\frac{3x_1 + a}{2y_1}\right)(x_1 - x_3) - y_1\right] mod\ p$$
$$= \left[\left(\frac{3(3)^2+1}{2(1)}\right)(3 - 3) - 1\right] (mod\ 17)$$
$$= \left[\left(\frac{28}{2}\right)(0) - 1\right] (mod\ 17)$$
$$= (-1) (mod\ 17)$$
$$= 16$$

Sehingga didapat $(x_3, y_3) = (3,16)$

Untuk mencari titik ketiga, tidak hanya menggunakan penjumlahan dua titik yang sama namun bisa menggunakan penjumlahan dua titik yang berbeda. Pada gambar 4.3 menjelaskan proses pembuatan titik ketiga di bidang terbatas f_p dengan penjumlahan dua titik yang berbeda. Pada proses pembuatan titik ketiga ini terdapat dua titik yang berbeda yakni

$P = (x_1, y_1)$ dan $Q = (x_2, y_2)$, untuk nilai $x_1, y_1, x_2, y_2, x_3, y_3 \in E(F_p)$.Syarat pertama untuk proses ini adalah P ≠ Q, jika syarat tersebut tidak terpenuhi maka kembali ke awal untuk x_1, y_1, x_2, y_2, jika syarat terpenuhi maka ke proses selanjutnya yakni melakukan penghitungan menggunakan rumus lamda pada persamaan (2.9). Setelah nilai lamda ditemukan, kemudian x_3 dapat dihitung dengan menggunakan persamaan (2.13). Selanjutnya y_3 dapat dihitung dengan menggunakan persamaan (2.14). Titik ketiga x_3, y_3 telah ditemukan dari proses diatas.



Gambar 4.3. Flowchart pembuatan titik ketiga dengan penjumlahan dua titik berbeda

Contoh perhitungan secara aljabar untuk pembuatan titik ketiga dengan titik awal beda, untuk persamaan kurva eliptik $E: y^2 = x^3 + x + 5$ dengan $a = 1,\ b = 5,\ p = 17$ didapatkan titik kurva eliptik

$$(x, y) = \begin{Bmatrix} (2,7), (2,10), (3,1), (3,16), (5,4), (5,13), (7,7), (7,10), \\ (8,7), (8,10), (11,2), (11,15), (14,3), (14,14) \end{Bmatrix}$$

Untuk $P = (x_1, y_1)$ dan $Q = (x_2, y_2)$ maka $P \neq Q = P + Q = R = (x_3, y_3)$ dimana :

$$x_3 = \left[\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - x_1 - x_2\right] mod\ p$$

$$y_3 = \left[\left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1\right] mod\ p$$

Ambil $P = (3,1)$ dan $Q = (8,10)$ maka $P + Q = R(x_3, y_3)$, perhitungannya seperti di bawah ini:

$$x_3 = \left[\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - x_1 - x_2\right] mod\ p$$

$$= \left[\left(\frac{10-1}{8-3}\right)^2 - 3 - 8\right] (mod\ 17)$$

$$= \left[\left(\frac{9}{5}\right)^2 - 11\right] (mod\ 17)$$

Karena $9 \times 5^{-1} (mod\ 17) = 9 \times 7 (mod\ 17) = 12$. Ini menghasilkan

$$= [12^2 - 11] (mod\ 17)$$

$$= 14$$

$$y_3 = \left[\left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1\right] mod\ p$$

$$= \left[\left(\frac{10-1}{8-3}\right)(3 - 14) - 1\right] (mod\ 17)$$

$$= \left[\left(\frac{9}{5}\right)(-11) - 1\right] (mod\ 17)$$

$$= [(12)(-11) - 1] (mod\ 17)$$

$$= -133 (mod\ 17)$$

$$= 3$$

Sehingga didapat $(x_3, y_3) = (14,3)$

4.2 Domain Parameter

Untuk melakukan proses enkripsi dan dekripsi citra, diperlukan kunci publik dan kunci privat. Terlebih dahulu dipilih jenis domain parameter kurva eliptik. Domain parameter yang dipilih yakni SEC 2 (*Standards Efficient Cryptography*) : *Recommended Elliptic Curve Domain Parameters*. Berikut adalah beberapa kunci yang direkomendasikan oleh SEC 2[1]:

4.2.1 Parameter secp112r1

Bilangan prima p

$$p = DB7C\ 2ABF62E3\ 5E668076\ BEAD208B$$

Koefisien a

$$a = DB7C\ 2ABF62E3\ 5E668076\ BEAD2088$$

Koefisien b

$$b = 659E\ F8BA0439\ 16EEDE89\ 11702B22$$

Titik Basis G

$$G = 020948\ 7239995A\ 5EE76B55\ F9C2F098$$

Order n

$$n = DB7C\ 2ABF62E3\ 5E7628DF\ AC6561C5$$

Kofaktor h

$$h = 01$$

4.2.2 Parameter secp112r2

Bilangan prima p

$$p = DB7C\ 2ABF62E3\ 5E668076\ BEAD208B$$

Koefisien a

$$a = 6127\ C24C05F3\ 8A0AAAF6\ 5C0EF02C$$

Koefisien b

$$b = 51DE\ F1815DB5\ ED74FCC3\ 4C85D709$$

Titik Basis G

$$G = 034BA3\ 0AB5E892\ B4E1649D\ D0928643$$

Order n

$$n = 36DF\ 0AAFD8B8\ D7597CA1\ 0520D04B$$

Kofaktor h

$$h = 04$$

4.2.3 Parameter secp128r1

Bilangan prima p

$p = FFFFFFFD\ FFFFFFFF\ FFFFFFFF\ FFFFFFFF$

Koefisien a

$a = FFFFFFFD\ FFFFFFFF\ FFFFFFFF\ FFFFFFFC$

Koefisien b

$b = E87579C1\ 1079F43D\ D824993C\ 2CEE5ED3$

Titik Basis G

$G = 03\ 161FF752\ 8B899B2D\ 0C28607C\ A52C5B86$

Order n

$n = FFFFFFFE\ 00000000\ 75A30D1B\ 9038A115$

Kofaktor h

$h = 01$

4.2.4 Pembuatan Kunci Publik dan Kunci Privat

Kunci publik pada algoritma ECC berupa sepasang bilangan minimal sepanjang 112 bit. Kunci tersebut didapat dari operasi $Q = d \cdot G$ dimana kunci privat = d, kunci publik = Q dan G = titik basis yang ada pada domain parameter yang digunakan.

4.3 Pembangkitan Kunci

Dari parameter yang sesuai dengan standarisasi SEC 2, diambil sebagian parameter untuk membangkitkan kunci publik dan kunci privat tersebut. Untuk membangkitkan kunci tersebut dapat menggunakan perhitungan $Q = d.G$ yang sesuai dengan aturan kurva eliptik. Jika kunci sudah dibangkitkan, langkah selanjutnya yakni proses enkripsi dan dekripsi citra. Algoritma pembangkit kunci ElGamal dengan kurva eliptik yakni [11]:

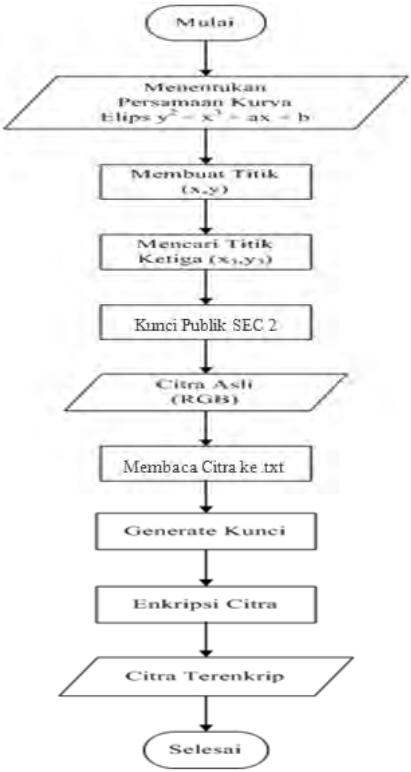
INPUT : Domain parameter $T(p, a, b, G, n, h)$
OUTPUT : $K_{publik} = Q$, $K_{privat} = d$
    Pilih $G = (x_1, y_1)$ sebagai titik pembangkit pada grup kurva eliptik $E(a, b)$
Pilih integer $d \in_R [1, n-1]$
Hitung $Q = d.G$
$K_{publik} = Q$, $K_{privat} = d$

4.4 Perancangan Sistem Enkripsi Citra

Di dalam perancangan sistem ini, citra asli berwarna (RGB) akan di enkrip dengan menggunakan algoritma EC-ElGamal. Terlebih dulu untuk memulai proses enkripsi yakni dengan menentukan persamaan kurva eliptik $y^2 = x^3 + ax + b$ (mod p), dengan memasukkan nilai a, b dan p untuk pemodulonya maka dari nilai tersebut dapat dihasilkan beberapa titik-titik yang sesuai dengan input yang dimasukkan. Nilai a, b dan p akan mempengaruhi $E(F_p)$.

Setelah menghasilkan beberapa titik tersebut, proses selanjutnya yakni mencari titik-titik ketiga (x_3, y_3), dimana titik ketiga ini adalah awal dari proses untuk membentuk sebuah kurva eliptik, yang nantinya titik ketiga ini dapat digunakan sebagai kunci publik. Namun pada tugas akhir ini, kunci publik yang digunakan tidak menggunakan proses secara manual seperti pada penjelasan perancangan sistem kurva eliptik di atas. Kunci publik yang digunakan berasal dari SEC (*Standards Efficient Cryptography*) 2 : *Recommended Elliptic Curve Domain Parameters* yang nanti pada sub bab berikutnya akan dijelaskan secara detail. Sama halnya kunci privat yang digunakan berasal dari SEC 2 juga.

Setelah didapatkan kunci publik dan kunci privat dari SEC 2, proses selanjutnya yakni memasukkan citra asli (RGB) ke dalam sistem ini. Proses selanjutnya yakni membangkitkan kunci *(generate key)*, dimana kunci publik akan disebarkan sedangkan kunci privat menjadi milik privasi. Kemudian citra asli berwarna tersebut dibaca piksel-pikselnya dalam bentuk *plaintext (.txt)*. Dan selanjutnya bisa dilakukan proses enkripsi citra asli tersebut untuk menghasilkan citra terenkrip dalam bentuk *chipertext (.txt)*.



Gambar 4.4. Diagram alir proses enkripsi citra

Citra asli *(M)* sebagai masukan algoritma enkripsi sistem kriptografi ElGamal dengan Kurva Eliptik. Pengenkripsi memilih secara acak integer k dan kemudian menghitungnya. Berikut adalah algoritma enkripsinya [11]:

INPUT : Domain parameter $T(p, a, b, G, n, h)$, kunci publik Q,
plaintext M
OUTPUT : *Chipertext* C_1, C_2
Pilih $k \in_R [1, n-1]$
Hitung $C_1 = k.G$
Hitung $C_2 = M + k.Q$
Chipertext C_1, C_2

4.5 Perancangan Sistem Dekripsi Citra

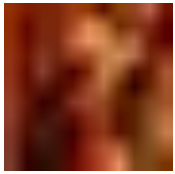
Pada perancangan sistem dekripsi ini, akan mengembalikan bentuk citra asli dari bentuk *chipertext* ke dalam bentuk *plaintext (.txt)* . Citra dalam bentuk *chipertext* tersebut kemudian diberikan kunci privat yang berasal dari SEC 2. Selanjutnya dilakukan proses dekripsi citra untuk mengembalikan citra dalam bentuk *plaintext*. Kemudian dilakukan proses pembacaan citra menjadi piksel-piksel dan menjadi citra asli. Berikut adalah algoritma dekripsinya [11] :

INPUT : Domain parameter $T(p, a, b, G, n, h)$, kunci privat d, chiper*text* (C_1, C_2)
OUTPUT : *plaintext M*
Hitung $M = C_2 - d.C_1$
plaintext M

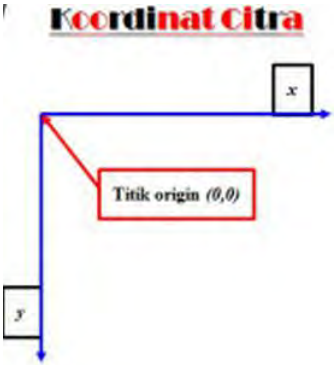
4.6 Matriks yang dibentuk dari Citra dengan Format .JPG

File citra dengan format .jpg (Joint Photographics Group) termasuk format file citra raster yang sering dipakai. Citra raster adalah citra yang bergantung pada resolusi. Resolusi merupakan sebuah ekspresi m x n dimana m adalah jumlah baris dan n adalah jumlah kolom. Resolusi juga mengacu pada jumlah pixel di dalam sebuah citra. Pada umumnya warna pada citra raster didefinisikan oleh tiga warrna dasar yaitu *red* (merah), *green* (hijau) dan *blue* (biru) atau disebut juga RGB *color*.

Berikut akan diberikan contoh citra format .jpg dengan ukuran 11 x 11 akan dibentuk matriks dari citra tersebut.



Gambar 4.5. Citra .jpg dengan ukuran 11 x 11



Gambar 4.6. Koordinat citra

Maka dapat dibentuk matriks dengan ukuran 11 x 11,

$$f(x,y)^{Red} = \begin{bmatrix} 149 & 96 & 138 & 144 & 146 & 140 & 115 & 154 & 190 & 194 & 102 \\ 147 & 92 & 129 & 123 & 163 & 215 & 150 & 132 & 150 & 153 & 39 \\ 149 & 95 & 122 & 133 & 186 & 227 & 221 & 171 & 165 & 89 & 49 \\ 156 & 99 & 160 & 142 & 152 & 142 & 181 & 214 & 187 & 63 & 141 \\ 157 & 97 & 160 & 101 & 35 & 99 & 210 & 163 & 55 & 71 & 177 \\ 161 & 103 & 100 & 25 & 83 & 146 & 200 & 115 & 27 & 128 & 158 \\ 174 & 80 & 37 & 49 & 127 & 187 & 192 & 100 & 61 & 147 & 164 \\ 172 & 49 & 55 & 74 & 85 & 191 & 176 & 63 & 101 & 146 & 209 \\ 163 & 35 & 70 & 43 & 36 & 147 & 163 & 46 & 105 & 126 & 215 \\ 158 & 26 & 50 & 48 & 43 & 150 & 213 & 190 & 111 & 148 & 174 \\ 151 & 19 & 35 & 39 & 92 & 180 & 193 & 242 & 122 & 148 & 113 \end{bmatrix}$$

$$f(x,y)^{Green} = \begin{bmatrix} 43 & 23 & 35 & 40 & 56 & 53 & 28 & 49 & 62 & 90 & 41 \\ 41 & 14 & 29 & 39 & 82 & 149 & 90 & 34 & 36 & 45 & 11 \\ 42 & 15 & 32 & 36 & 95 & 152 & 168 & 83 & 100 & 54 & 12 \\ 44 & 17 & 53 & 44 & 63 & 71 & 113 & 152 & 123 & 34 & 60 \\ 44 & 12 & 57 & 26 & 6 & 53 & 125 & 91 & 17 & 28 & 85 \\ 50 & 14 & 28 & 6 & 45 & 67 & 85 & 49 & 2 & 55 & 77 \\ 52 & 25 & 18 & 21 & 48 & 57 & 68 & 27 & 24 & 66 & 79 \\ 54 & 17 & 29 & 31 & 10 & 39 & 52 & 15 & 42 & 69 & 124 \\ 57 & 13 & 44 & 15 & 0 & 29 & 57 & 12 & 40 & 63 & 141 \\ 56 & 4 & 29 & 30 & 2 & 29 & 85 & 114 & 48 & 78 & 84 \\ 53 & 0 & 16 & 18 & 12 & 33 & 53 & 140 & 66 & 69 & 36 \end{bmatrix}$$

$$f(x,y)^{Blue} = \begin{bmatrix} 1 & 4 & 2 & 5 & 19 & 10 & 1 & 2 & 1 & 19 & 10 \\ 2 & 1 & 3 & 2 & 37 & 99 & 56 & 0 & 0 & 6 & 8 \\ 0 & 6 & 5 & 4 & 42 & 95 & 118 & 43 & 60 & 35 & 3 \\ 6 & 6 & 7 & 5 & 29 & 39 & 68 & 101 & 79 & 20 & 17 \\ 2 & 5 & 14 & 5 & 8 & 38 & 68 & 51 & 6 & 12 & 34 \\ 0 & 6 & 13 & 10 & 26 & 37 & 38 & 27 & 5 & 14 & 22 \\ 3 & 22 & 24 & 17 & 18 & 8 & 32 & 12 & 8 & 13 & 15 \\ 6 & 20 & 30 & 14 & 4 & 2 & 18 & 5 & 21 & 15 & 34 \\ 9 & 16 & 45 & 12 & 0 & 3 & 18 & 10 & 10 & 19 & 52 \\ 8 & 7 & 36 & 30 & 0 & 2 & 20 & 62 & 13 & 18 & 21 \\ 4 & 2 & 18 & 17 & 3 & 0 & 2 & 74 & 33 & 10 & 6 \end{bmatrix}$$

4.7 Pembuatan Program

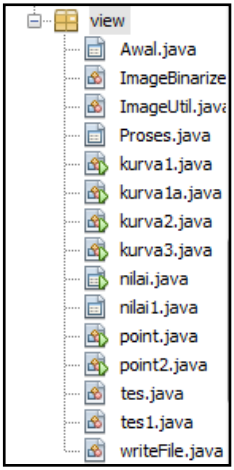
4.7.1 Pembuatan *Interface*

Untuk dapat mempermudah *user* dalam menggunakan program enkripsi dan dekripsi citra, maka dibuatlah *interface* sebagai berikut.

Gambar 4.7. *Interface* program

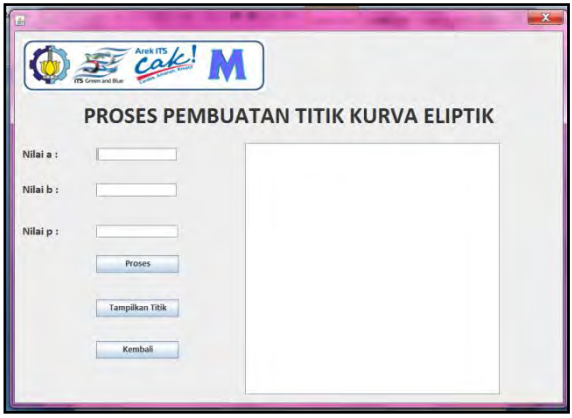
Selanjutnya, program enkripsi dan dekripsi citra pada tugas akhir ini akan diimplementasikan pada pemrograman JAVA

NETBEANS IDE 6.9.1. Pertama dibuat class-class seperti pada gambar berikut:



Gambar 4.8. Tampilan *class*

Setelah membuat class-class yang dibutuhkan, akan dibuat tampilan awal sebagai berikut.



Gambar 4.9. Tampilan awal

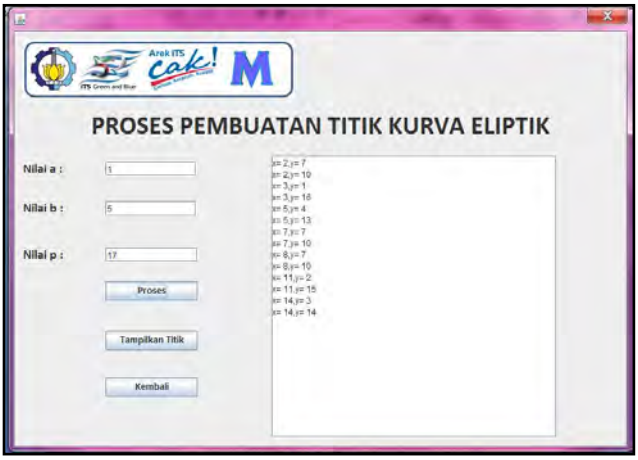
4.7.2 Pembuatan Titik Kurva Eliptik

Pada proses enkripsi dan dekripsi citra dengan menggunakan algoritma kurva eliptik yang mana untuk mendapatkan titik ketiga yang berfungsi sebagai kunci publik, maka diperlukan terlebih dahulu untuk mencari semua titik yang digunakan untuk mendapatkan titik ketiga tersebut. Pada program enkripsi dan dekripsi citra ini menggunakan metode kriptografi kurva eliptik pada bidang terbatas F_p yang perhitungannya sesuai dengan persamaan (2.2), yang mana $a, b \in F_p$, dan p adalah bilangan prima ganjil dan $p > 3$. Untuk perhitungan tersebut jika diterapkan dalam pemrograman java menjadi seperti berikut :

```
hasil1=(int) ((int) ( 4 * (Math.pow(a, 3)) + 27 * (Math.pow(b, 2))) % p);
hasil2=(int) 0 % p;

if(hasil1==hasil2)
{
    awl = new Awal();
    awl.setVisible(true);
}
else
    for(x=0;x<p;x++){
        for(y=0;y<p;y++){
            hasila=(int) Math.pow(y, 2)% p;
            hasilb=(int) (int) ((Math.pow(x, 3)+a*x+b)% p);
            if(hasila==hasilb){
                jTArea.append("x= "+x+","+"y= "+y+"\n");
```

Gambar 4.10. Listing program pembuatan titik kurva eliptik

Pada Gambar 4.10 menjelaskan bahwa nilai $a, b,$ dan p dimasukkan secara real akan menghasilkan banyak titik yang akan digunakan untuk membentuk titik kurva eliptik seperti pada gambar berikut :



Gambar 4.11. Tampilan awal untuk memasukkan nilai

4.7.3 Pembangkitan Titik Kurva Eliptik

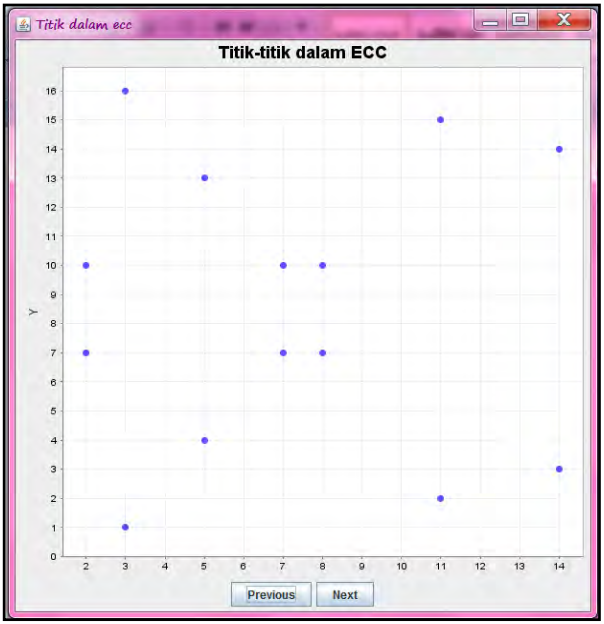
Setelah memasukkan nilai a, b, dan p maka langkah selanjutnya adalah membangkitkan titik-titik kurva eliptik tersebut. Berikut adalah listing program untuk membangkitkan titik kurva.

```
XYSeries series1 = new XYSeries("");
XYSeries series2 = new XYSeries("");
final long start = System.nanoTime();
hasil1 = (int) ((int) (4 * (Math.pow(a, 3)) + 27 * (Math.pow(b, 2))) % p);
hasil2 = (int) 0 % p;

if (hasil1 == hasil2) {
    awl = new Awal();
    awl.setVisible(true);
} else {
    for (x = 0; x < p; x++) {
        for (y = 0; y < p; y++) {
            hasila = (int) Math.pow(y, 2) % p;
            hasilb = (int) (int) ((Math.pow(x, 3) + a * x + b) % p);
            if (hasila == hasilb) {
                {series2.add(x, y);
```

Gambar 4.12. Listing program pembangkit titik kurva eliptik

Rumus pada persamaan (2.2) akan dimasukkan dalam program seperti pada gambar 4.12 yang digunakan untuk membangkitkan titik kurva yang telah dihasilkan pada listing program sebelumnya yang terdapat pada gambar 4.11.

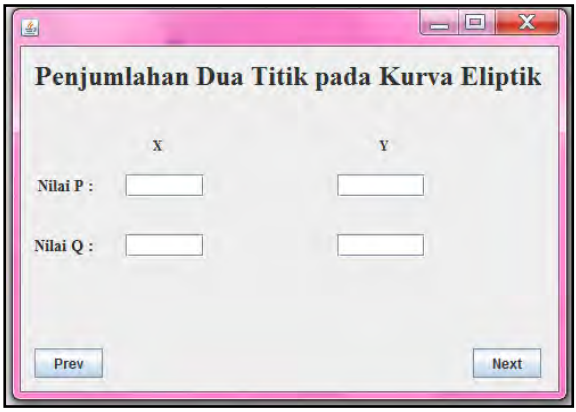
Pada gambar 4.13 menampilkan titik – titik kurva eliptik yang telah dibangkitkan dari proses program pada gambar 4.12.



Gambar 4.13. Tampilan titik – titik kurva eliptik

4.7.4 Pembuatan Titik Ketiga

Untuk pembuatan titik ketiga yang berguna untuk mencari kunci publik dapat dilakukan dengan dua cara yakni dengan pembuatan titik ketiga dengan titik awal yang sama dan pembuatan titik ketiga dengan titik awal yang berbeda. Sebelum penjelasan lebih lanjut, akan ditampilkan tampilan awal untuk membuat titik ketiga kurva eliptik. Berikut gambar tampilan awal titik ketiga :



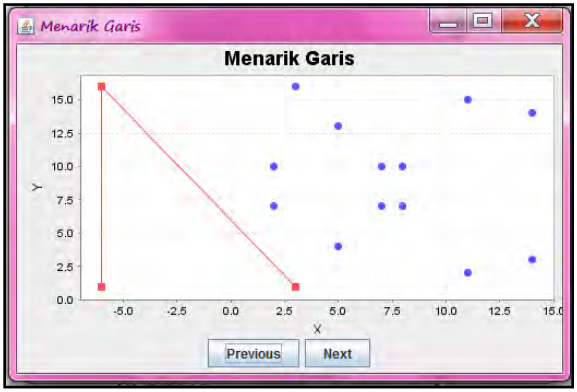
Gambar 4.14. Tampilan awal pembuatan titik ketiga

4.7.4.1 Pembuatan Titik Ketiga dengan Titik Awal Sama

Proses untuk membuat titik ketiga dengan titik awal yang sama dinamakan proses *doubling* atau penggandaan, yakni hanya satu titik lalu digandakan. Titik yang digunakan dalam proses *doubling* ini adalah titik – titik yang sama yang perhitungannya sesuai dengan persamaan (2.9) dan (2.10) untuk dapat menghasilkan x_3, y_3 seperti terlihat pada gambar 4.15 dan 4.16.

```
XYSeries series1 = new XYSeries("Series 1");
if (x1 == x2 & y1 == y2){
    delta1 = (((3*Math.pow(x1, 2) + a) / 2*y1))%p;
    delta1=(int)(delta1*3);
if (delta1 < 0)
    delta1 =  Math.abs(delta1);
    System.out.println("Nilainya"+delta1);
    x3=(long) (((Math.pow(delta1, 2)) - 2*x1)) ;
    x3 = x3 %= p;
    System.out.println("...x3 "+x3);

    y3=(long) ((delta1*(x1-x3)-y1))%p;
    if(y3<0 & y3>-p)
    y3=p+y3;
    System.out.println("...y3 "+y3);

    x4= x3;
    y4= p % -y3;
    System.out.println("..."+y4);
```

Gambar 4.15. Listing program pembuatan titik ketiga dengan titik awal sama



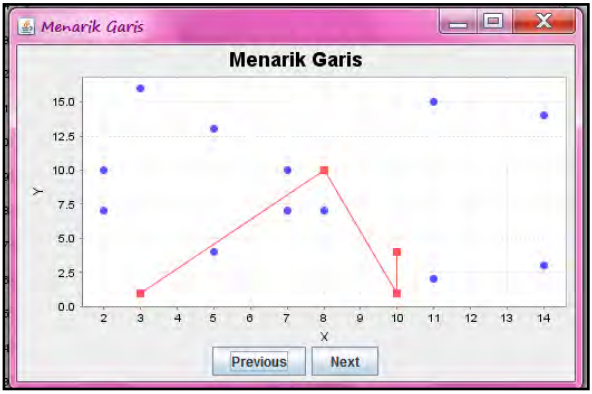
Gambar 4.16. Hasil tampilan titik ketiga dengan titik awal sama

4.7.4.2 Pembuatan Titik Ketiga dengan Titik Awal Berbeda

Proses untuk membuat titik ketiga dengan titik awal yang berbeda dinamakan proses *adding* atau penambahan, yakni dua titik lalu ditambahkan. Titik yang digunakan dalam proses *adding* ini adalah titik – titik yang berbeda yang perhitungannya sesuai dengan persamaan (2.7) dan (2.8) untuk dapat menghasilkan x_3, y_3 seperti terlihat pada gambar 4.17 dan 4.18.

```
delta1=(double) (y2 - y1) / (x2 - x1) % p;
if (delta1 < 0)
delta1=(int)(delta1*p);
if (delta1 < 0)
    delta1 =  Math.abs(delta1);
System.out.println("nilainya"+delta1);

x3=(long) (delta1 * delta1 - x1 - x2) % p;
System.out.println("...ht ht"+x3);
if(x3<0){
x3=(p+x3);
    System.out.println("...."+x3);
}
y3=(long) (delta1 * (x1 - x3) - y1);
y3=y3%p;
if(y3<0 & y3>-p)
y3=p+y3;
System.out.println("..."+y3);

x4= x3;
y4= p % -y3;
System.out.println("..."+y4);
}

series1.add(x1, y1);
series1.add(x2, y2);
series1.add(x4, y4);
series1.add(x3, y3);
```

Gambar 4.17. Listing program pembuatan titik ketiga dengan titik awal beda

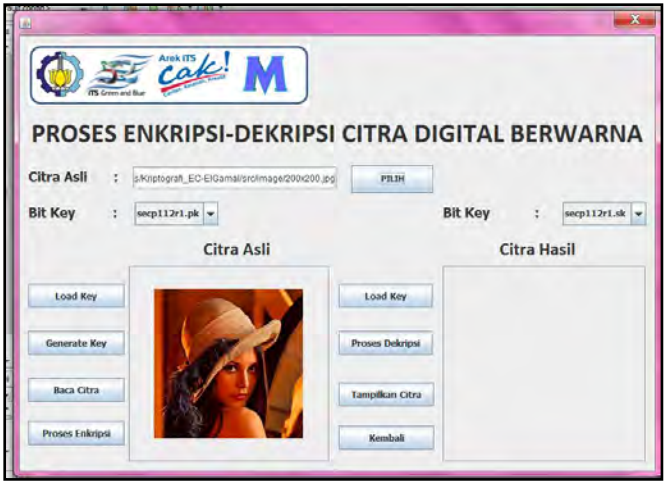


Gambar 4.18. Hasil tampilan titik ketiga dengan titik awal berbeda

4.7.5 Proses Enkripsi-Dekripsi Citra dengan Kriptografi Kurva Eliptik ElGamal

Setelah melakukan proses pembuatan titik dan titik ketiga kurva eliptik maka selanjutnya dilakukan proses enkripsi dan dekripsi pada citra digital berwarna. Berikut adalah tampilan awal dari proses enkripsi dan dekripsi citra digital berwarna.

Gambar 4.19. Tampilan awal proses enkripsi-dekripsi citra digital berwarna



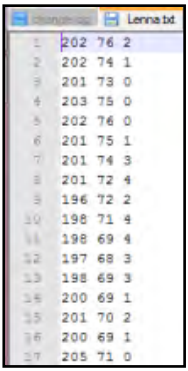
Gambar 4.20. Tampilan citra digital sebagai file input untuk proses enkripsi dan dekripsi citra

4.7.5.1 Pembacaan Citra Digital ke dalam File .txt

Pada tahap ini citra asli sebagai file input akan dibaca oleh program yang hasilnya berupa file .txt. Berikut adalah listing program pembacaan citra digital.

```
int indeks = 1;
for (int i = 0; i < kolom_citra; i++) {
    for (int j = 0; j < baris_citra; j++) {
        pixelAllRGB[i][j] = pict.get(i, j);
        String red = String.valueOf(pixelAllRGB[i][j].getRed());
        String green = String.valueOf(pixelAllRGB[i][j].getGreen());
        String blue = String.valueOf(pixelAllRGB[i][j].getBlue());
        String value = red + " " + green + " " + blue;
        try {
            data.writeToFile(value);
        } catch (IOException ex) {
            Logger.getLogger(Proses.class.getName()).log(Level.SEVERE, null, ex);
        }
    }
}
JOptionPane.showMessageDialog(null, "Citra Telah dibaca", "", JOptionPane.INFORMATION_MESSAGE);
System.out.println("Citra Telah dibaca");
```

Gambar 4.21. Listing program pembacaan citra digital ke dalam file .txt



Gambar 4.22. Potongan pembacaan file citra ke dalam format .txt

Pada gambar 4.22 di atas terlihat bahwa ada 3 kolom yang menerangkan piksel citra tersebut diisi oleh *Red* (R) di kolom pertama, *Green* (G) di kolom kedua dan *Blue* (B) di kolom ketiga. Dan pada baris nya menerangkan panjang RGB.

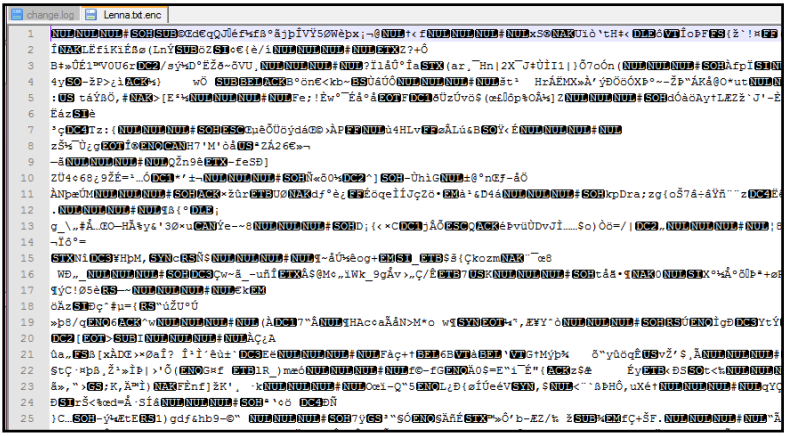
4.7.5.2 Proses Enkripsi Citra Digital Berwarna

Pada subbab ini adalah inti dari pengerjaan tugas akhir yakni proses enkripsi citra digital berwarna. Pada proses ini, citra digital berwarna sebagai file input yang telah dibaca oleh program ke dalam file .txt akan dilakukan proses enkripsi. Berikut adalah listing programnya.

```
final long start = System.nanoTime();
InputStream in = new FileInputStream(f);
OutputStream out = new CryptoOutputStream(new FileOutputStream(new File(f.getName() + ".enc")), cs, pk);

int read;
setStatus("Encrypting: " + f.getName() + " -> " + f.getName() + ".enc ...");
System.out.print("Encrypting: " + f.getName() + " -> " + f.getName() + ".enc ...");

int bytes = 0;
while ((read = in.read()) != -1) {
    out.write(read);
    bytes++;
}
out.flush();
in.close();
out.close();
setStatus("done");
System.out.println("OK");
JOptionPane.showMessageDialog(null, "Proses Enkripsi Berhasil", "", JOptionPane.INFORMATION_MESSAGE);
final long end = System.nanoTime();
System.out.println("Took: " + ((end - start) / 1000000) + "s");
```

Gambar 4.23. Listing program enkripsi citra digital

Setelah pengguna memasukkan file input berupa citra digital, maka selanjutnya dilakukan proses enkripsi. Berikut adalah hasil proses enkripsi dari file input citra digital yang berformat JPG menjadi file *chipertext* (,txt)



Gambar 4.24. Potongan kode hasil enkripsi citra dalam format .txt

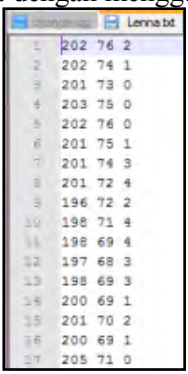
4.7.5.3 Proses Dekripsi Citra Digital Berwarna

Pada bagian ini, citra digital yang telah menjadi citra terenkrip kemudian dilakukan proses dekripsi atau pengembalian ke dalam bentuk semula (citra asli). Berikut adalah listing programnya.

```
final long start = System.nanoTime();
InputStream in = new CryptoInputStream(new FileInputStream(f), cs, sk);
OutputStream out = new FileOutputStream(new File(f.getName().substring(0, f.getName().length() - 4) + ".dec"));

System.out.print("Decrypting: " + f.getName() + " -> " + f.getName().substring(0, f.getName().length() - 4) + ".dec ...");
setStatus("Decrypting: " + f.getName() + " -> " + f.getName().substring(0, f.getName().length() - 4) + ".dec ...");

int bytes = 0;
int read;
while ((read = in.read()) != -1) {
    out.write(read);
    bytes++;
}
out.flush();
in.close();
out.close();
System.out.println("OK");
setStatus("done");
JOptionPane.showMessageDialog(null, "Proses Dekripsi Berhasil", "", JOptionPane.INFORMATION_MESSAGE);
final long end = System.nanoTime();
System.out.println("Took: " + ((end - start) / 1000000) + "s");
```

Gambar 4.25. Listing program dekripsi citra digital

Setelah pengguna mendapatkan hasil kode dari proses enkripsi citra, selanjutnya yakni mengembalikan file kode tersebut ke bentuk semula dengan menggunakan proses dekripsi.



Gambar 4.26. Potongan hasil dekripsi citra dalam format .txt

4.7.5.4 Proses Tampilan Citra Setelah Proses Dekripsi

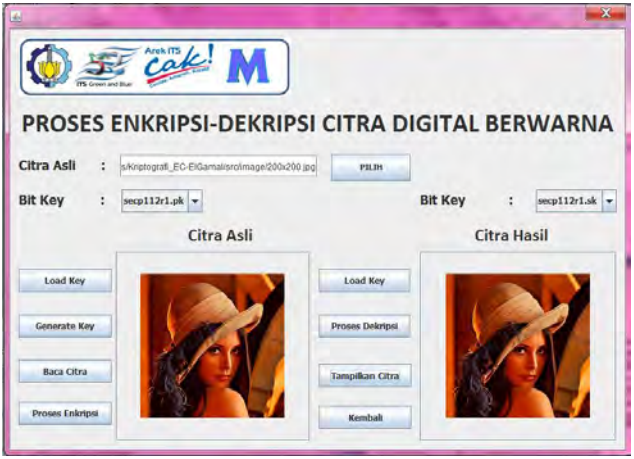
Pada subbab ini, citra digital hasil dari proses dekripsi citra akan ditampilkan dalam program Java. Berikut adalah listing programnya.

```
File readingFile = new File(f.getName().substring(0, f.getName().length() - 4));
BufferedReader reader;
if (f == null) {
    new JOptionPane("No file selected for encryption!");
    return;
}
try {
    long time = System.currentTimeMillis();
    final long start = System.nanoTime();
    reader = new BufferedReader(new FileReader(f));
    String readByte;
    int baris=1;
    while ((readByte = reader.readLine()) != null) {
        data = data + readByte + "\n";
        System.out.println("baris ke-"+baris+" sudah dibaca");
        baris++;
    }
    Sdata = data.split("\n"); // ==> tiap record berisi 1 baris rgb
    final long end = System.nanoTime();
    System.out.println("Took: " + ((end - start) / 1000000) + "s");
} catch (Exception ex) {
}
System.out.println("Read file finished");
```

```
int length = Sdata.length;// ==> banyaknya baris rgb / banyaknya pixel

int res[][] = new int[length][3];
String[][] Sres = new String[length][3];

//pisah tiap record menjadi 3
int c1, c2;
for (c1 = 0; c1 < length; c1++) {
    Sres[c1] = Sdata[c1].split(" ");
}
System.out.println("split RGB finished");
//convert ke integer
for (c1 = 0; c1 < length; c1++) {
    for (c2 = 0; c2 < 3; c2++) {
        res[c1][c2] = Integer.parseInt(Sres[c1][c2]);
    }
}
System.out.println("panjang rgb = "+length);
System.out.println("convert int finished");

BufferedImage img = createImage(res);
System.out.println("create image finished");
jLabel2.setIcon(new ImageIcon(img));
```

Gambar 4.27. Listing program tampilan citra setelah proses dekripsi

Setelah dilakukan proses dekripsi, maka selanjutnya yang dilakukan adalah mengembalikan file input citra yang semula merupakan file berformat .txt menjadi file citra hasil yang berformat .jpg dalam java.



Gambar 4.28. Tampilan citra hasil .jpg dari file format .txt

BAB V
UJI COBA DAN PEMBAHASAN

Pada bab ini berisi tentang hasil uji coba yang dihasilkan oleh sistem dan melakukan pembahasan terhadap hasil uji coba yang dilakukan.

5.1 Pengujian Titik Kurva Eliptik

Setelah dilakukan pembuatan titik kurva eliptik pada program, maka selanjutnya yang dilakukan adalah pengujian terhadap titik dengan data yang akan diambil berbeda – beda untuk nilai a, b dan p nya. Pada tabel 5.1 akan ditampilkan hasil pengujian titik kurva eliptik dengan nilai a, b, dan p yang berbeda.

Tabel 5.1. Pengujian titik kurva eliptik

No.	Nilai a, b dan p	Hasil Titik dalam program	No.	Nilai a, b dan p	Hasil Titik dalam program
1.	$a = 1,$ $b = 1,$ $p = 5$	x= 0,y= 1 x= 0,y= 4 x= 2,y= 1 x= 2,y= 4 x= 3,y= 1 x= 3,y= 4 x= 4,y= 2 x= 4,y= 3	2.	$a = 3,$ $b = 4,$ $p = 11$	x= 0,y= 2 x= 0,y= 9 x= 4,y= 5 x= 4,y= 6 x= 5,y= 1 x= 5,y= 10 x= 7,y= 4 x= 7,y= 7 x= 8,y= 1 x= 8,y= 10 x= 9,y= 1 x= 9,y= 10 x= 10,y= 0

3.	$a = 5,$ $b = 6,$ $p = 13$	x= 1,y= 5 x= 1,y= 8 x= 3,y= 3 x= 3,y= 10 x= 4,y= 5 x= 4,y= 8 x= 5,y= 0 x= 8,y= 5 x= 8,y= 8 x= 9,y= 0 x= 10,y= 4 x= 10,y= 9 x= 11,y= 1 x= 11,y= 12 x= 12,y= 0	4.	$a = 7,$ $b = 20,$ $p = 23$	x= 6,y= 5 x= 6,y= 18 x= 8,y= 6 x= 8,y= 17 x= 10,y= 3 x= 10,y= 20 x= 11,y= 5 x= 11,y= 18 x= 13,y= 10 x= 13,y= 13 x= 15,y= 2 x= 15,y= 21 x= 20,y= 8 x= 20,y= 15 x= 22,y= 9 x= 22,y= 14
5.	$a = 1,$ $b = 1,$ $p = 23$	x= 0,y= 1 x= 0,y= 22 x= 1,y= 7 x= 1,y= 16 x= 3,y= 10 x= 3,y= 13 x= 4,y= 0 x= 5,y= 4 x= 5,y= 19 x= 6,y= 4 x= 6,y= 19 x= 7,y= 11 x= 7,y= 12 x= 9,y= 7 x= 9,y= 16 x= 11,y= 3 x= 11,y= 20 x= 12,y= 4 x= 12,y= 19 x= 13,y= 7 x= 13,y= 16 x= 17,y= 3 x= 17,y= 20 x= 18,y= 3 x= 18,y= 20 x= 19,y= 5 x= 19,y= 18	6.	$a = 7,$ $b = 20,$ $p = 31$	x= 0,y= 12 x= 0,y= 19 x= 1,y= 11 x= 1,y= 20 x= 4,y= 9 x= 4,y= 22 x= 5,y= 5 x= 5,y= 26 x= 7,y= 3 x= 7,y= 28 x= 10,y= 6 x= 10,y= 25 x= 11,y= 8 x= 11,y= 23 x= 13,y= 13 x= 13,y= 18 x= 14,y= 14 x= 14,y= 17 x= 15,y= 11 x= 15,y= 20 x= 20,y= 10 x= 20,y= 21 x= 21,y= 2 x= 21,y= 29 x= 23,y= 14 x= 23,y= 17 x= 24,y= 0 x= 25,y= 14 x= 25,y= 17

Dari hasil pengujian pada tabel 5.1 , dapat dianalisa bahwa titik – titik yang dihasilkan dipengaruhi oleh nilai a, b dan p nya. Sehingga semakin besar nilai p nya maka titik yang dihasilkan pun semakin banyak. Karena nilai p merupakan nilai yang digunakan untuk membangkitkan titik-titik kurva tersebut.

5.2 Pengujian Program Enkripsi-Dekripsi Citra Digital Berwarna

5.2.1 Uji Coba dengan parameter secp112r1

a. Uji coba pertama

Ukuran citra asli : 50 x 50
Kunci publik : secp112r1.pk
Load key : (3882643937692781560491865929387986,
2491532865709098747886086209751444)
Waktu enkripsi : 11867 s
Kunci privat : secp112r1.sk
Load key : 213167027242699001022535748204823 9
(3882643937692781560491865929387986,
2491532865709098747886086209751444)
Waktu dekripsi : 7346 s
Panjang RGB : 2500

b. Uji coba kedua

Ukuran citra asli : 100 x 100
Kunci publik : secp112r1.pk
Load key : (3882643937692781560491865929387986,
2491532865709098747886086209751444)
Waktu enkripsi : 46355 s
Kunci privat : secp112r1.sk
Load key : 213167027242699001022535748204823 9
(3882643937692781560491865929387986,
2491532865709098747886086209751444)
Waktu dekripsi : 28336 s
Panjang RGB : 10000

c. Uji coba ketiga
Ukuran citra asli : 200 x 200
Kunci publik : secp112r1.pk
Load key : (3882643937692781560491865929387986,
2491532865709098747886086209751444)
Waktu enkripsi : 179225 s
Kunci privat : secp112r1.sk
Load key : 213167027242699001022535748204823 9
(3882643937692781560491865929387986,
2491532865709098747886086209751444)
Waktu dekripsi : 110467 s
Panjang RGB : 40000

d. Uji coba keempat
Ukuran citra asli : 300 x 300
Kunci publik : secp112r1.pk
Load key : (3882643937692781560491865929387986,
2491532865709098747886086209751444)
Waktu enkripsi : 416748 s
Kunci privat : secp112r1.sk
Load key : 213167027242699001022535748204823 9
(3882643937692781560491865929387986,
2491532865709098747886086209751444)
Waktu dekripsi : 250020 s
Panjang RGB : 90000

e. Uji coba kelima
Ukuran citra asli : 400 x 400
Kunci publik : secp112r1.pk
Load key : (3882643937692781560491865929387986,
2491532865709098747886086209751444)
Waktu enkripsi : 816792 s
Kunci privat : secp112r1.sk
Load key : 213167027242699001022535748204823 9
(3882643937692781560491865929387986,

249153286570909874788608620975144 4)
Waktu dekripsi : 468159 s
Panjang RGB : 160000

5.2.2 Uji Coba dengan parameter secp112r2

a. Uji coba pertama
Ukuran citra asli : 50 x 50
Kunci publik : secp112r2.pk
Load key : (590035393296490443607525777081453,
859600695549959319319474603730329)
Waktu enkripsi : 12122 s
Kunci privat : secp112r2.sk
Load key : 59395346312059203717035829055527 5
(590035393296490443607525777081453,
859600695549959319319474603730329)
Waktu dekripsi : 7863 s
Panjang RGB : 2500

b. Uji coba kedua
Ukuran citra asli : 100 x 100
Kunci publik : secp112r2.pk
Load key : (590035393296490443607525777081453,
859600695549959319319474603730329)
Waktu enkripsi : 46668 s
Kunci privat : secp112r2.sk
Load key : 59395346312059203717035829055527 5
(590035393296490443607525777081453,
859600695549959319319474603730329)
Waktu dekripsi : 29168 s
Panjang RGB : 10000

c. Uji coba ketiga
Ukuran citra asli : 200 x 200
Kunci publik : secp112r2.pk
Load key : (590035393296490443607525777081453,

859600695549959319319474603730329)
Waktu enkripsi : 184099 s
Kunci privat : secp112r2.sk
Load key : 59395346312059203717035829055527 5
(590035393296490443607525777081453,
859600695549959319319474603730329)
Waktu dekripsi : 111034 s
Panjang RGB : 40000

d. Uji coba keempat
Ukuran citra asli : 300 x 300
Kunci publik : secp112r2.pk
Load key : (590035393296490443607525777081453,
859600695549959319319474603730329)
Waktu enkripsi : 420484 s
Kunci privat : secp112r2.sk
Load key : 59395346312059203717035829055527 5
(590035393296490443607525777081453,
859600695549959319319474603730329)
Waktu dekripsi : 257053 s
Panjang RGB : 90000

e. Uji coba kelima
Ukuran citra asli : 400 x 400
Kunci publik : secp112r2.pk
Load key : (590035393296490443607525777081453,
859600695549959319319474603730329)
Waktu enkripsi : 834869 s
Kunci privat : secp112r2.sk
Load key : 59395346312059203717035829055527 5
(590035393296490443607525777081453,
859600695549959319319474603730329)
Waktu dekripsi : 651965 s
Panjang RGB : 90000

5.2.3 Uji Coba dengan parameter secp128r1

a. Uji coba pertama
   Ukuran citra asli : 50 x 50
   Kunci publik : secp128r2.pk
   Load key : (149756230064186907617027454885702804236,
   308761800057640715946280450798686262l0)
   Waktu enkripsi : 14830 s
   Kunci privat : secp128r1.sk
   Load key : 135608365238696490449859373000953748900
   (149756230064186907617027454885702804236,
   308761800057640715946280450798686262l0)
   Waktu dekripsi : 8805 s
   Panjang RGB : 2500

b. Uji coba kedua
   Ukuran citra asli : 100 x 100
   Kunci publik : secp128r2.pk
   Load key : (149756230064186907617027454885702804236,
   308761800057640715946280450798686262l0)
   Waktu enkripsi : 55434 s
   Kunci privat : secp128r1.sk
   Load key : 135608365238696490449859373000953748900
   (149756230064186907617027454885702804236,
   308761800057640715946280450798686262l0)
   Waktu dekripsi : 32375 s
   Panjang RGB : 10000

c. Uji coba ketiga
   Ukuran citra asli : 200 x 200
   Kunci publik : secp128r2.pk
   Load key : (149756230064186907617027454885702804236,
   308761800057640715946280450798686262l0)
   Waktu enkripsi : 228826 s
   Kunci privat : secp128r1.sk
   Load key : 135608365238696490449859373000953748900

(149756230064186907617027454885702804236,
308761800057640715946280450798686262l0)
Waktu dekripsi : 131166 s
Panjang RGB : 40000

d. Uji coba keempat
Ukuran citra asli : 300 x 300
Kunci publik : secp128r2.pk
Load key : (149756230064186907617027454885702804236,
308761800057640715946280450798686262l0)
Waktu enkripsi : 685978 s
Kunci privat : secp128r1.sk
Load key : 135608365238696490449859373000953748900
(149756230064186907617027454885702804236,
308761800057640715946280450798686262l0)
Waktu dekripsi : 308112 s
Panjang RGB : 90000

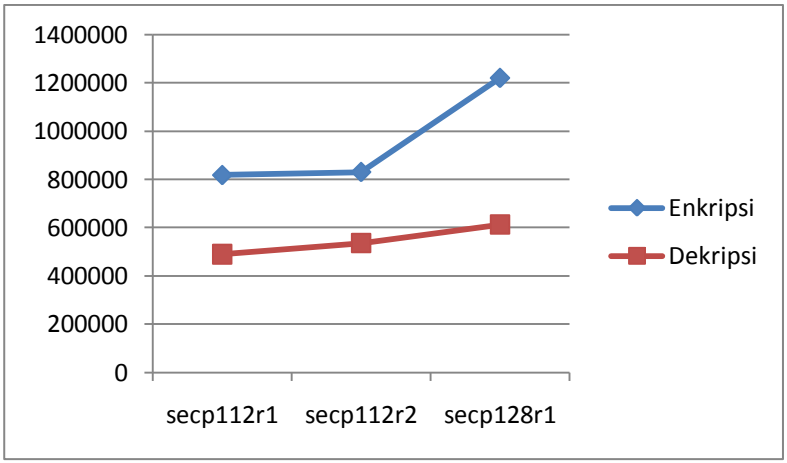
e. Uji coba kelima
Ukuran citra asli : 400 x 400
Kunci publik : secp128r2.pk
Load key : (149756230064186907617027454885702804236,
308761800057640715946280450798686262l0)
Waktu enkripsi : 1171129 s
Kunci privat : secp128r1.sk
Load key : 135608365238696490449859373000953748900
(149756230064186907617027454885702804236,
308761800057640715946280450798686262l0)
Waktu dekripsi : 660318 s
Panjang RGB : 160000

Tabel 5.2. Hasil uji coba program

Ukuran Kunci	Percobaan ke -	Ukuran Citra	Waktu Enkripsi (s)	Waktu Dekripsi (s)
secp112r1	1	50 × 50	11867	7346
	2	100 × 100	46355	28336
	3	200 × 200	179225	110467
	4	300 × 300	416748	250020
	5	400 × 400	816792	468159
		Rata-rata	**817553**	**489800**
secp112r2	1	50 × 50	12122	7863
	2	100 × 100	46668	29168
	3	200 × 200	184099	111034
	4	300 × 300	420484	257053
	5	400 × 400	834869	651965
		Rata-rata	**830346**	**535511**
secp128r1	1	50 × 50	14830	8805
	2	100 × 100	55434	32375
	3	200 × 200	228826	131166
	4	300 × 300	685978	308112
	5	400 × 400	1171129	660318
		Rata-rata	**1219294**	**612522**

Dapat dilihat pada tabel, uji coba dilakukan dengan total 15 kali percobaan dengan ukuran citra yang berbeda-beda pada setiap kunci bitnya. Untuk proses enkripsi pada bit kecil dengan ukuran citra yang kecil menghasilkan waktu enkripsi yang memiliki rata-rata kecil juga. Sedangkan untuk proses enkripsi dengan ukuran citra yang cukup besar pada bit yang cukup besar mempunyai rata-rata waktu yang besar yang artinya proses tersebut membutuhkan waktu yang cukup lama. Sama halnya dengan proses dekripsi dengan ukuran citra yang berbeda dan kunci bit yang berbeda. Hal ini disebabkan karena semakin tinggi kunci yang dipakai maka kunci publik dan kunci privat pun semakin panjang sehingga membutuhkan waktu yang cukup

lama. Selain itu juga disebabkan oleh semakin besar ukuran citra maka akan semakin lama dalam proses enkripsi maupun dekripsinya karena bergantung pada piksel citra yang diproses. Namun, dengan semakin tingginya kunci yang dipakai untuk proses enkripsi dan dekripsi maka pesan citra digital tersebut memiliki tingkat keamanan yang cukup tinggi, hanya saja memiliki kelemahan waktu komputasi yang cukup lama.



Gambar 5.1. Grafik rata-rata waktu proses enkripsi-dekripsi

BAB VI
PENUTUP

6.1 Kesimpulan

Berdasarkan hasil perancangan sistem dan uji coba program, dapat diambil beberapa kesimpulan sebagai berikut:

1. Dari hasil pengujian titik kurva eliptik terlihat titik-titik yang dihasilkan dipengaruhi oleh nilai a, b dan p nya. Sehingga semakin besar nilai p nya maka titik yang dihasilkan pun semakin banyak. Karena nilai p merupakan nilai yang digunakan untuk membangkitkan titik-titik kurva tersebut.
2. Untuk proses enkripsi dan dekripsi pada bit kecil dengan ukuran citra yang kecil, menghasilkan waktu enkripsi dan dekripsi yang memiliki rata-rata kecil juga. Sedangkan untuk proses enkripsi dengan ukuran citra yang cukup besar pada bit yang cukup besar mempunyai rata-rata waktu yang besar yang artinya proses tersebut membutuhkan waktu yang cukup lama.
3. Semakin tinggi kunci yang dipakai maka kunci publik dan kunci privat pun semakin panjang sehingga membutuhkan waktu yang cukup lama.
4. Semakin tingginya kunci yang dipakai untuk proses enkripsi dan dekripsi maka pesan citra digital tersebut memiliki tingkat keamanan yang cukup tinggi, hanya saja memiliki kelemahan waktu komputasi yang cukup lama.

6.2 Saran

Berdasarkan hasil yang sudah dicapai pada tugas akhir ini, terdapat beberapa hal yang perlu dipertimbangkan untuk pengembangannya antara lain:

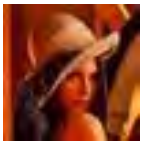
1. Program enkripsi-dekripsi ini masih bersifat statis, sehingga untuk melakukan uji coba dengan variabel berbeda harus diganti secara manual maka untuk penelitian selanjutnya diharapkan bersifat dinamis agar program lebih

mempermudah user dalam melakukan proses enkripsi-dekripsi citra.

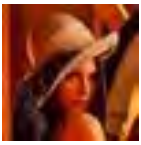
2. Mengembangkan dengan file input citra berbagai ukuran dan format.

Lampiran

(a) Citra asli lenna.jpg



(b) Citra hasil lenna



(c) Matriks 50 × 50 dalam pembacaan citra di .txt

Matriks $f(x,y)^{Red} =$

Kolom 1 – 16, Baris 1 – 25

202	197	158	86	93	99	97	101	114	130	140	145	148	144	144	152
196	196	159	86	90	97	94	101	117	127	137	141	141	141	146	146
194	196	160	85	90	96	94	100	114	122	131	137	137	141	145	145
198	200	164	85	88	97	96	102	118	125	134	140	144	149	142	148
205	207	167	81	81	94	97	105	119	130	136	141	146	148	146	141
210	209	161	73	77	92	94	98	113	122	129	137	143	142	122	118
210	208	160	72	78	93	94	97	110	120	126	135	146	125	111	117
211	205	156	72	81	94	93	98	110	120	129	137	128	110	118	119
211	205	156	73	80	94	94	98	112	122	128	132	111	112	120	117
207	205	158	73	79	92	94	95	109	117	139	118	110	113	116	123
205	206	158	71	76	90	94	95	109	115	172	112	109	113	125	137
208	208	156	68	74	92	96	102	105	132	190	98	107	119	130	131
211	213	161	74	80	98	99	102	106	157	175	98	107	118	131	128
215	221	163	74	81	98	98	98	97	173	182	102	100	112	124	126
218	221	165	76	81	96	98	98	97	189	205	138	106	113	123	152
217	218	165	77	80	91	96	99	97	195	215	171	109	111	148	148
219	221	171	74	80	91	96	96	96	208	228	192	137	132	138	137
223	223	173	74	79	93	99	97	91	197	248	177	139	110	131	145
222	222	176	74	77	92	96	98	84	166	254	180	138	120	143	130
221	222	176	74	77	91	96	97	96	120	238	212	141	136	128	127
222	224	177	74	78	92	95	96	109	98	179	243	147	117	123	126
219	225	179	74	79	95	96	98	112	104	158	224	118	115	129	115
219	225	178	73	80	97	98	98	118	120	139	181	112	130	96	43
220	226	182	75	80	98	99	100	117	123	132	144	135	109	43	25
220	226	181	78	80	98	99	101	110	137	133	82	118	60	30	31

Kolom 17 – 32, Baris 1 – 25

151	146	147	145	141	138	139	143	140	139	136	135	135	131	121	106
145	146	144	136	134	134	133	138	139	138	138	135	130	128	121	109
144	140	137	133	130	127	122	124	130	138	136	131	130	131	119	105
149	144	142	147	160	168	160	152	134	122	129	131	126	126	118	106
131	134	141	150	170	184	190	198	200	175	127	115	123	121	114	104
120	123	128	139	164	184	193	203	211	219	200	138	97	107	108	101
124	126	131	137	153	180	199	210	214	214	214	217	187	102	91	97
119	128	140	143	154	185	202	200	209	224	231	234	250	190	72	81
126	137	151	152	152	173	188	217	232	228	226	229	232	242	171	75
141	145	149	134	142	187	218	221	217	220	227	231	231	230	249	190
146	140	126	138	190	214	208	212	221	223	224	229	230	227	233	250
133	128	154	197	200	199	204	215	214	213	222	228	230	230	226	235
126	160	180	181	200	204	207	201	198	211	219	223	216	213	224	223
154	168	160	183	195	192	193	197	204	200	208	209	203	209	212	206
158	151	169	168	185	191	197	200	196	195	199	202	205	201	192	183
144	162	158	164	177	189	185	184	188	183	189	195	193	182	177	186
152	137	149	159	149	130	124	141	148	162	160	145	140	171	197	214
136	134	146	132	105	73	65	96	58	51	40	24	111	201	219	214
130	143	130	93	61	39	45	51	46	27	32	112	192	207	208	203
131	111	74	35	32	25	42	44	46	38	131	207	202	193	186	196
110	60	42	26	33	30	28	31	41	97	187	208	188	183	187	209
50	21	29	39	36	41	11	53	102	153	201	177	177	193	227	246
24	20	22	29	44	36	44	154	187	160	195	173	195	224	246	252
26	36	23	28	28	40	139	195	195	170	184	203	222	232	247	248
24	25	22	37	31	115	196	189	195	153	143	152	191	228	241	240

Kolom 33 – 50, Baris 1 – 10

101	155	196	196	196	194	190	180	173	181	245	244	122	94	107	108	111	123
102	146	190	194	189	193	189	186	179	169	203	255	211	99	104	109	116	108
104	140	175	184	188	190	187	193	183	171	166	230	255	160	88	108	102	41
103	136	165	171	180	186	189	180	174	163	161	186	253	235	112	81	29	13
99	139	164	163	173	182	176	171	168	164	162	163	206	255	177	17	11	26
95	144	180	170	160	173	173	173	173	166	168	165	175	223	83	4	27	32
90	148	196	179	133	131	177	178	171	169	173	175	178	75	3	21	24	23
86	150	193	182	123	65	149	182	173	170	172	180	106	7	20	22	21	21
74	145	194	184	129	31	84	173	178	166	179	137	20	17	26	21	22	22
64	139	190	182	130	31	31	116	166	162	158	44	12	27	25	20	20	35

Kolom 33 – 50, Baris 11 – 25

134	119	192	183	134	30	8	103	208	217	101	3	22	23	21	20	22	104
209	136	191	189	119	42	126	219	241	252	143	3	20	22	21	20	82	151
222	202	189	183	149	186	233	233	223	242	151	5	19	18	17	48	146	164
201	197	201	210	225	229	227	222	222	247	114	0	15	20	36	125	165	174
178	195	216	225	220	217	221	212	196	220	61	5	20	21	87	161	170	176
204	219	214	212	216	223	222	181	160	156	16	15	15	48	146	164	174	173
214	208	213	221	229	233	189	117	153	111	6	17	18	97	163	171	172	169
206	216	225	231	191	132	90	126	158	31	16	19	44	146	167	175	171	167
206	214	189	136	104	117	174	158	31	13	22	21	93	164	178	174	166	162
201	140	69	75	164	224	155	26	14	24	20	38	131	170	180	174	168	161
227	147	57	75	140	115	15	18	26	23	22	69	129	183	179	176	172	166
248	210	59	38	114	34	13	28	24	20	37	108	142	171	177	174	175	172
255	238	94	16	100	42	22	30	21	19	64	136	160	149	150	155	161	165
255	252	143	10	85	54	23	26	22	25	102	159	175	166	162	148	132	133
247	215	117	16	71	66	24	26	22	45	127	174	173	168	171	163	147	136

Kolom 1 – 16, Baris 26 – 50

223	228	186	75	79	99	97	101	132	179	156	73	53	39	38	30
227	230	181	81	82	98	94	88	185	181	88	31	31	42	44	16
225	234	190	86	97	111	87	96	155	86	29	36	34	48	56	19
226	237	193	91	98	117	132	98	37	22	56	40	29	54	60	28
224	236	193	91	93	118	97	52	33	48	51	25	25	42	45	66
217	227	193	90	95	110	65	62	39	47	43	25	16	26	46	111
217	230	196	88	97	101	59	53	40	50	57	19	20	57	96	77
217	232	198	94	89	89	51	50	41	48	65	32	24	38	55	6
215	231	198	87	86	93	43	42	36	43	66	52	60	22	66	104
220	232	202	86	94	89	46	34	30	43	50	74	58	71	152	128
224	233	195	96	98	82	32	24	40	54	50	50	87	183	156	92
224	238	195	94	95	70	34	25	56	57	52	58	124	175	140	45
219	232	194	78	78	49	32	24	57	66	55	69	92	162	69	11
215	229	191	76	57	36	26	25	44	50	62	75	88	60	7	19
216	225	186	107	65	26	34	19	46	65	45	68	82	70	27	20
213	219	195	100	44	19	33	34	37	63	59	59	56	79	71	29
213	220	196	120	35	22	45	45	40	39	51	41	68	81	63	57
217	226	199	112	16	28	24	36	29	29	38	39	63	79	75	82
219	227	201	91	24	24	15	43	30	26	36	50	53	83	63	74
221	222	201	82	22	21	22	49	26	25	21	38	54	77	81	82
218	219	196	77	11	21	27	38	23	21	25	34	47	77	64	61
217	224	200	93	16	26	22	27	24	23	25	37	46	58	59	49
211	222	203	89	19	21	26	26	24	21	23	40	52	34	51	47
208	224	195	76	18	23	24	22	28	22	21	26	64	69	44	16
209	227	192	67	17	20	20	21	30	26	26	31	37	66	41	12

Kolom 17 – 32, Baris 26 – 50

21	29	24	20	91	197	210	157	92	84	78	71	127	197	235	239
25	22	23	34	158	210	179	76	36	36	125	100	120	177	244	167
18	20	14	105	201	182	135	146	120	120	191	185	131	169	236	160
18	13	63	183	186	114	168	200	198	182	186	187	160	169	232	215
12	25	137	193	80	129	180	206	228	224	220	203	180	168	227	229
36	67	198	91	40	138	176	200	217	228	221	196	170	159	216	230
38	130	134	11	59	132	171	192	202	208	210	176	156	153	204	234
106	165	31	18	77	128	167	187	195	202	201	170	141	133	179	219
120	64	12	30	86	133	165	185	190	202	202	191	170	177	204	201
71	20	31	34	81	134	169	181	188	187	189	188	192	227	233	183
26	27	37	33	60	116	160	175	187	159	137	152	153	165	163	141
14	23	31	37	44	78	130	148	176	182	157	158	180	193	175	124
23	25	30	32	36	52	91	128	164	174	179	176	179	181	153	50
30	27	21	28	29	40	43	76	131	158	182	208	212	193	104	12
33	23	20	22	31	34	49	76	111	134	162	191	194	183	136	38
30	26	19	22	28	30	59	126	147	154	169	175	176	210	237	219
26	29	19	21	29	42	51	117	138	160	173	174	191	217	231	243
28	27	17	23	31	80	56	120	153	172	177	184	199	209	223	234
48	31	19	25	37	99	58	128	171	177	180	188	194	203	218	226
51	34	29	23	65	121	69	139	175	176	179	185	190	201	210	222
48	52	32	30	104	131	76	151	176	178	176	181	188	196	206	217
24	34	19	53	131	108	93	174	183	181	176	176	185	196	199	209
21	21	29	87	132	70	130	177	187	186	183	178	181	192	197	207
18	19	61	122	89	83	170	178	185	188	187	180	179	183	193	202
12	36	95	88	68	145	176	180	184	187	190	185	181	182	189	197

Kolom 33 – 50, Baris 26 – 35

146	62	58	26	58	77	25	25	15	75	148	176	168	166	162	159	154	152
35	74	31	16	56	90	25	20	25	109	163	171	160	164	160	159	150	143
103	108	43	21	54	95	25	21	43	133	170	166	157	161	157	153	140	125
164	111	70	25	50	101	26	16	70	149	169	160	157	152	148	141	121	134
187	152	91	25	45	108	23	24	108	165	163	153	153	146	142	124	135	220
181	153	77	24	40	113	28	40	136	171	159	153	149	141	133	126	206	254
175	139	43	26	36	110	38	67	153	169	157	152	146	136	121	165	249	251
169	104	19	35	33	105	59	104	164	157	148	147	144	136	128	212	255	250
156	59	8	38	31	88	91	145	165	155	147	146	141	129	145	240	254	252
124	24	18	47	33	70	118	158	163	151	143	143	141	125	157	250	254	255

Kolom 33 – 50, Baris 36 – 50

71	10	30	48	35	56	142	166	155	148	141	139	138	122	170	254	254	253
21	13	33	51	41	56	161	165	152	151	143	135	131	119	183	255	253	254
11	27	36	58	46	58	167	155	148	149	147	134	125	107	181	255	255	253
17	28	36	65	49	64	164	149	144	139	139	129	118	102	193	255	253	255
5	20	37	65	52	75	146	104	111	116	124	122	111	107	223	255	254	254
142	38	22	59	47	82	136	112	100	92	89	90	85	99	235	255	253	214
255	214	79	33	39	85	151	140	124	114	95	79	93	110	238	255	217	79
247	255	239	72	19	98	157	140	138	126	111	98	113	173	255	255	133	46
243	252	255	194	20	103	155	143	134	129	115	105	166	238	255	222	84	74
237	255	255	255	79	100	153	141	131	120	106	129	245	255	255	166	76	94
232	245	252	255	147	105	147	131	121	119	104	157	253	255	232	123	87	96
224	241	255	255	221	123	120	128	129	122	115	154	213	255	197	95	82	72
220	234	250	255	255	114	57	78	91	99	137	155	181	253	147	69	66	71
213	231	246	253	255	142	59	59	40	23	84	203	233	219	64	47	65	71
209	224	239	249	255	189	74	82	63	31	78	240	215	92	31	57	67	53

Matriks $f(x,y)^{Green} =$

Kolom 1 – 16, Baris 1 – 25

74	68	42	19	22	22	20	23	34	37	40	44	40	42	43	38
72	68	43	17	18	22	21	25	34	37	37	39	39	39	42	42
69	68	42	13	16	23	22	24	31	36	37	39	37	37	41	39
69	69	42	11	14	22	21	24	31	34	36	36	37	36	36	35
72	68	41	7	11	18	18	24	29	32	33	32	36	35	46	47
73	67	37	3	8	16	15	19	27	28	31	32	33	39	38	40
73	69	37	4	11	17	14	18	26	29	33	30	35	31	30	37
75	70	37	4	13	18	15	16	26	30	31	34	28	29	31	37
73	70	36	5	12	16	14	14	24	28	33	31	27	28	31	34
70	70	35	5	10	14	16	16	24	27	39	22	24	25	31	39
71	68	35	3	7	12	14	16	23	29	61	16	22	27	34	44
74	70	35	4	7	12	11	16	23	48	70	14	27	30	35	37
75	75	38	6	11	19	12	14	20	69	57	16	22	27	33	33
79	81	40	2	8	19	15	14	20	83	58	16	21	24	30	35
81	81	42	2	6	17	14	14	17	90	67	30	19	25	33	51
80	77	43	3	6	12	8	10	12	87	72	38	17	27	44	46
82	80	44	2	6	13	9	7	13	108	87	51	28	40	41	43
83	80	44	2	8	15	12	10	8	107	109	39	36	33	38	46
81	79	45	2	6	12	11	11	3	80	122	52	41	33	40	38
80	79	45	2	6	11	8	9	7	44	129	86	41	39	34	36
82	81	46	2	4	7	6	7	18	11	98	119	40	34	39	40
82	84	46	2	5	7	7	7	20	15	82	114	26	32	35	27
82	84	45	1	6	9	7	7	23	21	49	81	20	35	20	4
83	85	47	4	6	9	8	10	22	23	27	38	35	31	9	7
83	88	48	4	5	10	8	6	17	33	39	23	35	11	11	15

Kolom 17 – 32, Baris 1 – 25

37	40	39	36	38	42	44	41	43	42	38	39	39	38	39	31
37	36	31	31	36	40	41	40	42	39	38	39	38	40	39	32
35	33	29	29	35	38	38	34	36	38	38	38	37	39	35	34
34	45	53	64	86	100	92	79	54	33	35	39	36	36	33	31
45	60	68	77	96	110	122	132	137	104	47	25	32	32	31	26
42	51	56	64	82	105	123	132	142	154	138	74	22	25	29	26
42	47	52	56	70	99	127	136	141	147	159	173	139	41	18	22
39	45	51	55	66	93	119	127	147	171	181	183	199	138	12	14
41	51	55	58	60	81	112	151	170	168	166	174	180	195	126	22
48	54	48	41	59	109	145	151	150	159	172	176	178	179	198	143
47	47	40	58	110	128	125	136	154	158	166	173	175	178	188	207
39	38	69	99	104	114	122	140	138	146	154	162	171	175	176	189
37	64	80	87	103	114	119	113	121	134	147	158	149	147	169	172
56	60	66	83	99	100	99	107	112	117	130	129	130	143	148	141
53	59	69	72	87	93	96	103	104	99	108	120	131	130	121	114
48	56	60	69	77	87	88	88	87	88	93	103	106	100	99	107
49	48	56	62	59	54	64	70	69	74	76	69	69	88	117	144
42	45	49	48	40	26	31	58	31	21	12	8	57	124	154	151
40	45	40	27	21	9	18	25	22	8	12	57	112	135	141	138
38	29	18	7	6	7	14	14	25	23	71	129	131	119	119	130
31	12	11	4	13	6	3	6	25	62	115	132	117	112	119	128
10	3	7	9	16	17	1	16	53	104	128	106	104	101	126	143
4	2	2	3	17	19	14	72	102	106	127	93	80	104	138	148
6	7	2	4	9	19	59	95	129	106	89	77	86	106	133	142
4	3	2	11	10	48	105	109	121	58	36	43	77	93	113	128

Kolom 33 – 50, Baris 1 – 10

29	55	72	67	69	64	61	62	60	63	140	153	45	28	34	35	37	39
28	44	68	71	67	65	63	63	63	54	87	173	123	28	33	35	41	33
30	42	60	66	66	65	63	63	60	54	52	127	187	77	21	35	33	14
28	43	54	58	62	60	60	59	54	49	46	68	171	154	33	19	3	1
25	42	52	52	56	57	54	53	50	47	47	44	99	191	87	0	2	1
23	41	56	50	44	51	51	48	48	48	47	46	53	107	33	0	5	8
22	40	61	54	34	34	51	50	49	46	46	51	45	8	1	1	2	1
19	41	60	57	28	7	41	52	46	47	45	48	19	1	1	3	3	1
7	43	58	55	27	1	21	48	45	43	46	27	1	1	1	1	0	2
10	35	56	55	29	1	1	22	51	43	33	5	0	1	1	2	0	10

Kolom 33 – 50, Baris 11 – 25

86	27	57	53	29	0	0	65	150	149	49	0	2	1	1	2	2	47
171	48	56	56	18	13	92	168	189	203	110	2	0	0	3	0	33	69
178	134	52	57	81	134	178	177	171	190	108	0	1	4	0	18	67	74
142	146	107	131	161	174	168	170	169	191	73	2	1	2	4	52	73	75
115	131	155	165	161	162	168	145	123	155	33	0	0	0	35	71	75	78
133	152	154	150	158	168	169	100	78	90	5	0	0	13	61	74	78	75
149	146	156	166	172	178	117	40	85	69	1	1	2	40	71	77	76	74
151	155	164	166	128	66	18	56	91	12	0	0	15	63	76	79	76	75
143	154	125	80	33	32	80	82	7	1	2	0	38	76	83	82	80	80
133	75	27	42	70	91	70	7	0	3	0	10	59	80	86	84	82	77
130	54	12	46	65	38	0	0	0	1	2	27	64	89	85	86	81	80
148	90	0	14	57	5	0	2	4	0	9	49	71	85	85	84	83	82
163	128	9	2	51	12	2	1	1	0	28	69	79	72	76	77	79	81
160	157	35	0	38	17	0	2	2	3	49	78	85	81	81	76	71	71
135	105	24	0	33	27	0	2	2	17	58	79	79	78	85	80	75	73

Kolom 1 – 16, Baris 26 – 50

84	88	48	3	4	12	6	7	38	55	47	23	11	14	17	11
86	88	49	3	8	9	3	15	88	59	19	7	9	17	22	2
86	94	52	5	14	18	19	37	76	38	17	15	9	25	37	5
88	97	57	6	14	24	50	41	7	3	36	19	10	35	41	8
84	90	54	8	13	35	43	23	7	26	28	3	7	21	21	24
82	85	51	5	20	36	29	23	12	31	25	0	2	2	11	44
82	85	52	9	30	36	23	22	21	39	37	1	2	12	28	29
82	88	57	14	15	19	19	25	22	29	48	7	3	14	15	1
78	90	58	7	8	25	12	20	14	26	54	32	12	4	33	47
80	93	59	5	19	22	21	9	4	14	27	49	18	33	92	51
85	94	58	19	23	23	10	4	19	31	21	31	30	109	81	32
88	95	65	21	25	21	13	6	39	44	27	35	47	74	54	15
87	93	59	7	19	12	12	2	41	54	42	36	41	76	18	0
84	91	54	5	12	11	5	1	27	30	49	52	37	21	1	1
80	85	56	36	22	6	2	1	33	42	24	57	60	42	17	2
75	83	67	27	15	5	7	13	15	43	43	42	39	51	46	7
77	83	62	47	7	2	19	20	10	20	29	20	51	60	37	27
85	87	65	45	0	7	3	10	4	10	15	13	41	62	47	48
85	89	62	25	6	4	1	23	10	8	11	25	28	62	48	49
86	93	65	24	2	2	6	28	6	1	2	18	33	61	63	63
83	91	67	23	0	3	7	10	2	2	6	12	32	61	46	37
79	88	66	26	1	6	4	3	3	3	5	13	30	46	37	29
78	88	64	22	1	3	5	5	4	2	5	21	33	19	27	26
76	88	65	17	2	1	4	2	2	2	1	8	49	49	20	0
77	94	66	19	1	1	1	3	4	5	6	5	17	47	20	1

Kolom 17 – 32, Baris 26 – 50

6	13	5	4	34	106	139	87	24	12	16	5	20	58	106	120
7	8	6	8	76	139	105	8	0	11	86	36	11	37	120	77
2	1	0	45	121	110	36	37	28	39	102	67	19	36	139	75
0	1	16	97	110	18	39	67	66	62	68	71	36	28	135	123
0	4	61	117	23	13	40	66	90	98	94	67	41	24	126	137
12	23	117	48	0	21	33	50	74	91	84	56	35	20	104	138
7	65	75	0	3	14	33	43	57	68	71	42	23	21	80	148
56	83	11	2	9	16	27	37	51	59	62	37	18	9	50	105
53	27	0	6	17	15	23	32	43	52	64	56	37	61	101	82
23	0	1	4	15	16	24	30	33	41	46	50	56	110	123	69
7	1	2	3	7	12	24	26	38	27	15	16	21	40	36	30
0	3	1	3	2	7	16	24	36	38	22	9	24	49	47	28
2	4	2	0	2	2	6	23	30	35	41	42	48	50	44	7
1	1	3	0	3	1	2	8	19	33	50	69	79	67	22	1
3	1	1	2	1	3	3	14	23	33	42	60	65	71	60	17
1	2	1	0	4	1	4	26	34	37	42	44	51	96	139	135
2	2	1	1	3	0	8	25	28	37	39	38	62	95	119	132
9	1	3	2	3	6	7	25	32	38	37	45	63	80	100	112
23	1	3	1	1	8	9	28	32	34	38	45	55	70	90	108
23	0	3	1	7	17	10	29	35	36	36	41	53	68	79	101
19	13	4	0	12	20	12	32	38	39	33	38	47	60	73	92
2	6	4	2	13	15	17	35	39	37	33	36	43	55	68	82
1	0	0	8	19	7	28	37	41	40	35	35	42	50	63	76
2	0	3	14	8	15	35	35	37	40	39	32	34	44	58	68
2	2	7	7	7	29	36	37	37	39	40	35	33	40	52	63

Kolom 33 – 50, Baris 26 – 35

47	4	4	0	23	29	0	1	1	27	68	77	73	73	76	77	75	76
0	27	1	0	22	32	0	1	4	46	74	75	70	70	71	73	74	72
36	31	1	1	19	37	1	0	14	62	76	72	71	70	73	71	69	63
46	16	6	0	17	44	0	0	29	66	75	71	72	71	71	69	61	70
56	28	7	0	11	52	1	2	44	72	74	70	70	70	67	62	68	116
54	29	6	0	9	52	4	10	59	77	73	68	65	67	64	62	105	124
50	25	1	2	5	52	10	24	69	76	72	71	70	68	62	84	124	125
43	17	0	1	1	51	21	40	74	75	72	69	68	68	60	110	127	149
36	12	2	3	1	43	35	55	75	72	67	70	68	65	72	119	145	164
25	4	3	3	0	34	48	63	75	71	69	69	68	61	76	134	163	165

Kolom 33 – 50, Baris 36 – 50

14	0	2	2	0	25	57	66	75	70	73	69	68	57	82	161	173	168
3	1	3	5	1	21	66	71	76	73	71	69	69	57	97	182	179	179
1	3	2	9	2	20	73	74	77	76	75	70	66	53	113	193	184	180
1	2	4	12	1	19	74	73	77	75	74	71	65	51	133	193	174	178
1	0	6	10	2	23	59	38	45	57	67	67	63	58	154	176	164	150
88	20	1	8	0	26	56	47	36	31	29	30	40	49	145	158	156	100
156	139	47	1	0	26	65	67	60	51	40	27	25	40	148	165	109	17
136	167	168	40	0	34	70	70	65	63	57	52	37	77	172	154	44	0
131	158	190	136	2	36	71	68	64	62	57	47	69	137	177	113	9	6
128	158	175	181	42	34	73	68	65	58	50	56	152	171	162	55	2	16
124	156	173	184	93	40	76	67	64	62	48	71	157	168	118	24	10	14
112	145	165	180	142	50	61	65	68	68	58	57	92	161	76	6	7	4
98	134	165	175	172	42	8	22	37	50	64	53	86	152	37	1	5	13
88	122	158	172	180	73	4	6	0	2	34	93	127	104	3	1	10	18
78	106	144	167	181	117	22	26	10	1	27	124	89	21	1	10	19	5

Matriks $f(x,y)^{Blue} =$

Kolom 1 – 16, Baris 1 – 25

0	2	3	3	4	4	0	1	0	6	4	2	2	2	0	4
0	3	4	2	3	3	2	2	4	3	1	1	1	1	3	3
2	3	2	1	3	4	0	1	1	1	1	4	1	0	2	0
3	1	3	2	3	3	0	2	3	3	1	1	5	2	0	3
3	1	3	4	3	2	1	5	3	5	2	1	3	1	10	13
3	1	3	3	3	3	2	2	4	0	2	2	0	8	4	4
1	2	4	3	3	4	3	3	2	2	2	1	7	5	1	2
1	2	3	3	4	4	3	2	2	4	2	3	2	2	4	0
1	4	2	4	3	3	5	4	4	2	1	3	3	0	1	4
0	2	2	4	3	2	6	3	3	1	7	6	1	1	2	3
0	3	2	2	2	2	5	1	0	4	15	2	3	4	5	1
1	5	4	2	1	3	4	3	2	11	17	3	4	0	3	1
0	3	4	5	4	6	2	2	3	21	7	4	2	6	6	3
1	4	0	3	2	2	0	3	2	23	7	1	4	0	4	4
1	4	1	1	1	2	3	4	6	22	5	4	2	5	6	7
2	5	4	2	3	5	4	2	7	15	6	7	2	3	5	6
2	1	1	3	3	3	2	1	7	32	5	6	5	3	6	5
4	1	2	3	4	5	5	3	4	31	16	3	5	3	5	4
2	0	3	3	2	3	4	4	2	29	21	3	8	3	7	0
1	0	1	3	2	2	4	5	0	18	34	12	7	6	8	7
3	2	2	3	1	2	2	3	0	1	33	21	6	2	5	15
2	4	3	3	4	3	3	2	5	0	33	35	1	2	7	3
1	2	2	2	3	5	4	2	5	2	15	29	0	5	4	5
2	3	2	2	3	5	3	2	4	0	5	14	19	9	7	7
3	0	5	3	2	0	5	2	0	4	11	15	19	7	13	16

Kolom 17 – 32, Baris 1 – 25

0	0	3	3	3	0	0	1	1	0	3	1	1	4	2	2
1	3	1	1	1	2	2	3	0	0	2	1	1	4	2	2
2	1	1	0	3	4	2	0	0	4	1	5	4	2	0	2
5	14	21	30	49	61	53	38	19	1	1	2	1	2	4	0
10	25	35	42	59	71	77	80	83	60	14	0	5	2	1	3
6	13	18	25	44	64	74	80	87	98	87	36	0	1	0	5
5	6	9	13	26	52	77	87	86	94	105	124	99	13	0	1
2	3	7	9	18	44	69	76	98	119	128	130	142	99	1	0
4	4	5	7	9	34	62	101	119	116	114	120	130	141	84	14
4	9	6	0	19	60	92	92	98	105	118	122	126	122	143	101
5	3	5	23	59	77	71	78	99	102	116	122	119	122	133	156
5	3	28	50	54	60	72	83	88	93	107	112	113	121	125	139
7	14	21	36	50	64	71	65	69	82	97	104	94	95	115	119
9	11	14	31	51	49	45	54	61	65	81	78	79	93	100	99
5	12	19	22	42	44	42	48	53	51	64	72	82	86	79	75
6	8	13	21	25	39	45	37	35	34	43	56	61	63	60	64
6	8	12	19	24	31	40	42	36	34	40	37	41	46	64	85
4	3	7	14	20	16	32	57	36	19	11	8	29	68	100	98
5	6	5	11	22	9	23	28	22	12	11	27	59	77	89	84
5	7	5	6	9	5	13	12	30	20	37	80	77	74	67	80
16	8	9	6	14	6	6	9	28	58	67	83	71	68	74	81
2	3	9	9	17	17	0	8	36	71	77	64	63	52	74	85
5	2	4	2	22	25	3	32	61	70	80	42	23	44	74	85
7	9	1	4	13	16	22	36	79	68	41	18	26	47	71	80
5	5	3	12	9	21	48	58	72	26	2	12	27	27	50	65

Kolom 33 – 50, Baris 1 – 10

5	5	2	2	0	6	4	0	4	2	33	46	3	2	2	0	2	2
0	4	5	4	2	4	4	3	2	0	12	61	34	0	1	0	2	4
3	3	3	5	1	1	1	3	1	1	0	32	76	11	2	2	4	7
5	2	1	2	0	2	2	2	2	0	2	4	61	49	2	4	2	1
0	0	2	0	2	3	3	3	2	4	2	1	17	73	24	0	3	4
1	0	4	0	3	2	2	0	2	0	2	3	2	32	10	0	7	6
3	1	5	0	3	2	3	1	0	2	1	0	2	0	4	3	4	3
2	2	1	3	0	3	3	3	1	3	0	0	2	1	3	0	3	2
0	3	0	0	2	0	6	2	4	0	1	2	3	4	4	0	3	3
0	0	5	4	1	3	3	0	6	1	1	0	0	4	1	2	4	5

Kolom 33 – 50, Baris 11 – 25

63	2	1	3	0	0	0	44	102	102	25	0	4	3	0	2	3	20
132	10	0	0	0	15	65	113	132	145	79	0	1	7	0	2	16	22
131	95	0	7	46	94	122	120	111	130	73	1	0	4	0	10	28	22
102	103	55	75	100	110	112	112	117	134	53	0	0	0	5	20	24	18
74	83	100	103	105	105	114	90	70	101	21	0	2	0	14	21	21	15
77	97	102	101	108	112	115	45	31	55	3	0	0	9	22	21	18	14
93	95	101	110	117	121	67	10	48	45	0	1	2	13	22	25	16	16
97	101	109	110	84	34	4	30	62	6	1	0	11	21	31	21	20	24
90	102	81	47	11	1	26	48	5	1	3	1	17	30	35	31	33	32
84	45	15	33	19	16	29	3	0	0	0	7	21	30	34	34	33	30
75	23	7	32	33	10	0	1	0	3	3	15	26	35	33	33	26	29
88	40	2	10	38	7	0	1	6	1	6	15	29	36	34	32	32	30
99	67	2	2	34	2	3	3	0	2	14	24	26	28	31	29	31	35
99	91	9	0	28	8	6	2	3	5	18	25	25	27	34	26	27	32
72	52	7	1	22	12	0	2	3	6	19	15	15	25	24	26	25	29

Kolom 1 – 16, Baris 26 – 50

3	1	1	4	1	3	3	7	13	4	8	12	12	17	22	13
4	2	1	0	5	3	2	9	37	12	3	5	11	23	25	0
1	0	5	2	6	3	10	21	46	26	19	22	12	31	41	4
0	0	5	0	3	6	26	30	9	5	45	26	6	41	47	7
5	4	0	4	2	17	43	27	8	29	34	5	7	28	21	10
1	3	3	2	15	23	29	24	17	42	25	3	2	2	9	18
1	4	2	4	24	30	25	27	25	47	39	1	2	6	15	15
1	2	4	7	6	7	22	31	24	35	56	10	0	12	15	0
0	2	0	0	4	14	17	23	17	34	58	33	2	0	24	30
1	2	1	1	14	14	24	12	7	18	37	55	16	22	58	33
2	1	6	13	17	17	12	5	26	39	26	33	23	74	49	22
2	3	13	15	17	16	12	8	49	51	33	41	37	44	19	7
2	2	4	3	15	6	11	4	44	68	52	43	37	43	1	1
2	2	0	1	7	7	4	1	37	39	59	60	33	16	1	0
2	0	6	30	16	7	3	0	40	48	29	65	62	39	16	2
2	7	20	18	7	5	6	8	17	52	44	48	45	48	41	9
0	3	9	28	6	4	22	23	10	22	32	25	59	65	36	19
0	6	12	26	1	4	2	13	8	12	21	16	44	68	46	36
0	1	3	11	6	5	1	25	12	6	15	28	31	67	45	44
4	2	3	13	4	4	7	27	5	1	4	20	38	64	61	59
2	4	9	13	1	1	6	7	1	4	8	15	37	64	42	35
4	2	3	9	4	7	4	3	0	5	4	13	33	48	39	28
1	3	5	6	1	1	4	4	5	4	5	23	35	16	27	25
1	2	3	9	5	3	6	3	3	3	2	8	54	50	16	0
3	3	7	7	1	3	3	3	3	4	7	6	18	49	19	0

Kolom 17 – 32, Baris 26 – 50

1	13	7	4	15	49	83	53	11	0	5	6	2	3	40	64
7	8	12	7	38	83	68	5	0	14	69	24	4	1	58	40
3	3	0	19	68	72	7	0	5	18	70	31	0	3	86	36
0	3	8	48	74	6	0	11	17	12	28	24	2	1	93	72
2	3	25	68	16	0	5	7	27	37	35	15	0	0	84	86
2	10	72	29	0	4	1	0	6	23	16	5	3	0	67	87
4	27	45	0	4	2	5	1	4	6	6	4	4	0	44	97
29	46	2	2	6	2	2	2	1	3	3	2	3	1	19	51
26	19	0	6	10	3	1	1	0	2	2	1	2	24	60	26
19	2	3	2	3	6	3	3	2	0	2	1	4	56	70	19
3	0	0	3	3	3	2	2	5	4	2	4	8	22	17	2
0	5	3	4	4	1	6	0	3	3	2	2	11	22	12	4
1	3	1	1	1	3	3	1	3	2	4	4	4	8	1	1
3	2	1	1	4	6	0	5	5	1	2	12	20	17	0	0
1	3	3	1	1	1	3	3	1	5	5	8	10	21	34	14
3	0	0	3	2	5	0	2	4	2	1	2	3	36	78	73
2	7	0	0	4	2	2	4	3	3	2	0	4	28	55	60
5	4	3	1	0	3	0	5	3	3	1	2	3	14	33	37
19	0	3	1	3	5	4	5	1	2	2	1	0	5	19	34
22	1	4	3	6	4	2	2	2	3	4	6	1	3	9	32
15	14	3	0	1	1	3	2	1	0	1	4	2	0	6	28
5	5	1	1	3	7	3	2	2	0	1	1	3	2	0	15
0	0	4	3	3	2	5	2	2	1	5	1	1	4	2	8
2	2	2	4	4	2	3	1	1	2	3	2	3	1	2	5
1	1	5	3	2	4	3	3	3	1	3	2	3	2	0	2

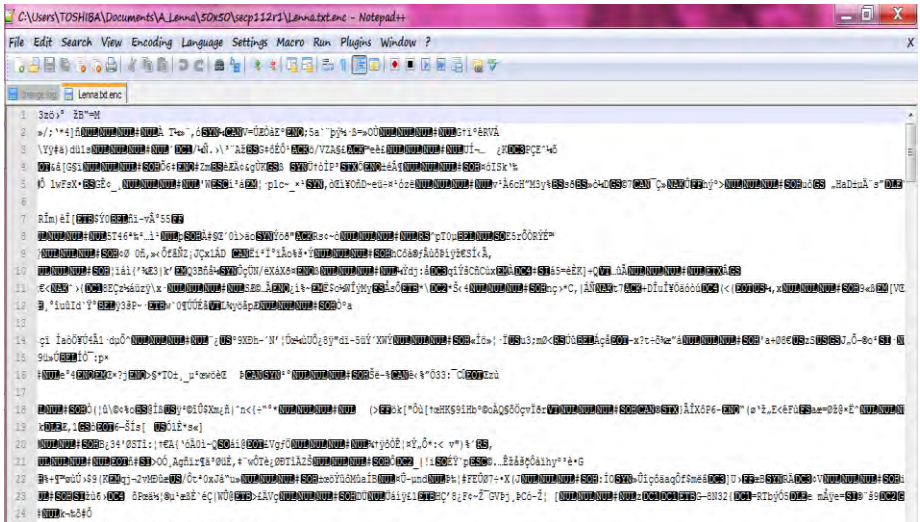
Kolom 33 – 50, Baris 26 – 35

15	0	4	0	17	17	0	1	1	13	17	10	5	12	15	17	19	27
4	19	0	1	12	20	2	3	3	13	14	14	7	9	11	14	24	28
17	23	5	2	13	23	0	1	8	18	14	10	12	15	11	21	23	22
8	0	4	0	12	25	3	1	9	16	11	11	15	16	19	21	24	24
4	2	5	3	9	29	3	4	8	11	14	16	16	18	25	23	23	19
0	3	2	0	7	31	4	0	7	13	12	13	18	20	22	26	13	0
2	0	2	2	3	32	7	5	7	9	8	16	18	21	22	21	4	5
2	0	1	2	2	27	12	4	11	15	14	20	16	21	21	12	0	33
2	6	2	1	1	24	12	3	12	18	16	20	13	19	21	2	24	56
2	3	0	2	0	18	12	9	11	18	20	24	17	15	10	11	49	53

Kolom 33 – 50, Baris 36 – 50

3	3	1	4	1	20	16	6	14	21	26	20	17	15	8	42	66	62
1	3	5	5	1	17	18	7	24	25	21	21	18	16	22	67	74	78
0	3	3	4	1	11	21	18	25	25	25	32	22	15	42	84	80	77
2	3	5	4	1	13	24	21	25	27	32	33	25	20	60	82	69	70
0	0	4	3	1	12	14	3	11	15	24	28	27	25	61	55	50	37
52	16	0	4	1	9	7	5	1	2	3	6	11	16	33	35	43	12
76	82	26	2	2	10	14	14	12	10	9	6	2	6	38	53	21	2
57	91	104	29	0	9	16	19	12	20	19	18	1	16	54	40	2	3
55	84	124	86	2	7	9	11	13	17	17	10	1	29	56	18	3	3
59	97	112	116	24	0	14	17	15	19	13	13	48	47	46	2	3	3
59	90	106	118	55	8	30	21	21	19	13	12	34	52	22	1	4	3
49	84	102	118	85	9	21	22	24	22	15	2	9	43	7	2	4	3
33	74	101	112	108	17	1	5	11	17	13	4	18	34	2	2	4	2
21	55	95	109	113	42	1	0	0	1	7	4	18	15	2	3	3	4
8	36	86	107	118	67	1	3	2	1	6	13	4	1	3	2	5	3

(d) Potongan kode hasil enkripsi citra digital di .txt



(e) Matriks 50 × 50 dari hasil dekripsi citra digital

Matriks $f(x,y)^{Red} =$

Kolom 1 – 16, Baris 1 – 25

202	197	158	86	93	99	97	101	114	130	140	145	148	144	144	152
196	196	159	86	90	97	94	101	117	127	137	141	141	141	146	146
194	196	160	85	90	96	94	100	114	122	131	137	137	141	145	145
198	200	164	85	88	97	96	102	118	125	134	140	144	149	142	148
205	207	167	81	81	94	97	105	119	130	136	141	146	148	146	141
210	209	161	73	77	92	94	98	113	122	129	137	143	142	122	118
210	208	160	72	78	93	94	97	110	120	126	135	146	125	111	117
211	205	156	72	81	94	93	98	110	120	129	137	128	110	118	119
211	205	156	73	80	94	94	98	112	122	128	132	111	112	120	117
207	205	158	73	79	92	94	95	109	117	139	118	110	113	116	123
205	206	158	71	76	90	94	95	109	115	172	112	109	113	125	137
208	208	156	68	74	92	96	102	105	132	190	98	107	119	130	131
211	213	161	74	80	98	99	102	106	157	175	98	107	118	131	128
215	221	163	74	81	98	98	98	97	173	182	102	100	112	124	126
218	221	165	76	81	96	98	98	97	189	205	138	106	113	123	152
217	218	165	77	80	91	96	99	97	195	215	171	109	111	148	148
219	221	171	74	80	91	96	96	96	208	228	192	137	132	138	137
223	223	173	74	79	93	99	97	91	197	248	177	139	110	131	145
222	222	176	74	77	92	96	98	84	166	254	180	138	120	143	130
221	222	176	74	77	91	96	97	96	120	238	212	141	136	128	127
222	224	177	74	78	92	95	96	109	98	179	243	147	117	123	126
219	225	179	74	79	95	96	98	112	104	158	224	118	115	129	115
219	225	178	73	80	97	98	98	118	120	139	181	112	130	96	43
220	226	182	75	80	98	99	100	117	123	132	144	135	109	43	25
220	226	181	78	80	98	99	101	110	137	133	82	118	60	30	31

Kolom 17 – 32, Baris 1 – 10

151	146	147	145	141	138	139	143	140	139	136	135	135	131	121	106
145	146	144	136	134	134	133	138	139	138	138	135	130	128	121	109
144	140	137	133	130	127	122	124	130	138	136	131	130	131	119	105
149	144	142	147	160	168	160	152	134	122	129	131	126	126	118	106
131	134	141	150	170	184	190	198	200	175	127	115	123	121	114	104
120	123	128	139	164	184	193	203	211	219	200	138	97	107	108	101
124	126	131	137	153	180	199	210	214	214	214	217	187	102	91	97
119	128	140	143	154	185	202	200	209	224	231	234	250	190	72	81
126	137	151	152	152	173	188	217	232	228	226	229	232	242	171	75
141	145	149	134	142	187	218	221	217	220	227	231	231	230	249	190

Kolom 17 – 32, Baris 11 – 25

146	140	126	138	190	214	208	212	221	223	224	229	230	227	233	250
133	128	154	197	200	199	204	215	214	213	222	228	230	230	226	235
126	160	180	181	200	204	207	201	198	211	219	223	216	213	224	223
154	168	160	183	195	192	193	197	204	200	208	209	203	209	212	206
158	151	169	168	185	191	197	200	196	195	199	202	205	201	192	183
144	162	158	164	177	189	185	184	188	183	189	195	193	182	177	186
152	137	149	159	149	130	124	141	148	162	160	145	140	171	197	214
136	134	146	132	105	73	65	96	58	51	40	24	111	201	219	214
130	143	130	93	61	39	45	51	46	27	32	112	192	207	208	203
131	111	74	35	32	25	42	44	46	38	131	207	202	193	186	196
110	60	42	26	33	30	28	31	41	97	187	208	188	183	187	209
50	21	29	39	36	41	11	53	102	153	201	177	177	193	227	246
24	20	22	29	44	36	44	154	187	160	195	173	195	224	246	252
26	36	23	28	28	40	139	195	195	170	184	203	222	232	247	248
24	25	22	37	31	115	196	189	195	153	143	152	191	228	241	240

Kolom 33 – 50, Baris 1 – 25

134	119	192	183	134	30	8	103	208	217	101	3	22	23	21	20	22	104
209	136	191	189	119	42	126	219	241	252	143	3	20	22	21	20	82	151
222	202	189	183	149	186	233	233	223	242	151	5	19	18	17	48	146	164
201	197	201	210	225	229	227	222	222	247	114	0	15	20	36	125	165	174
178	195	216	225	220	217	221	212	196	220	61	5	20	21	87	161	170	176
204	219	214	212	216	223	222	181	160	156	16	15	15	48	146	164	174	173
214	208	213	221	229	233	189	117	153	111	6	17	18	97	163	171	172	169
206	216	225	231	191	132	90	126	158	31	16	19	44	146	167	175	171	167
206	214	189	136	104	117	174	158	31	13	22	21	93	164	178	174	166	162
201	140	69	75	164	224	155	26	14	24	20	38	131	170	180	174	168	161
227	147	57	75	140	115	15	18	26	23	22	69	129	183	179	176	172	166
248	210	59	38	114	34	13	28	24	20	37	108	142	171	177	174	175	172
255	238	94	16	100	42	22	30	21	19	64	136	160	149	150	155	161	165
255	252	143	10	85	54	23	26	22	25	102	159	175	166	162	148	132	133
247	215	117	16	71	66	24	26	22	45	127	174	173	168	171	163	147	136
101	155	196	196	196	194	190	180	173	181	245	244	122	94	107	108	111	123
102	146	190	194	189	193	189	186	179	169	203	255	211	99	104	109	116	108
104	140	175	184	188	190	187	193	183	171	166	230	255	160	88	108	102	41
103	136	165	171	180	186	189	180	174	163	161	186	253	235	112	81	29	13
99	139	164	163	173	182	176	171	168	164	162	163	206	255	177	17	11	26
95	144	180	170	160	173	173	173	173	166	168	165	175	223	83	4	27	32
90	148	196	179	133	131	177	178	171	169	173	175	178	75	3	21	24	23
86	150	193	182	123	65	149	182	173	170	172	180	106	7	20	22	21	21
74	145	194	184	129	31	84	173	178	166	179	137	20	17	26	21	22	22
64	139	190	182	130	31	31	116	166	162	158	44	12	27	25	20	20	35

Kolom 1 – 16, Baris 26 – 50

223	228	186	75	79	99	97	101	132	179	156	73	53	39	38	30
227	230	181	81	82	98	94	88	185	181	88	31	31	42	44	16
225	234	190	86	97	111	87	96	155	86	29	36	34	48	56	19
226	237	193	91	98	117	132	98	37	22	56	40	29	54	60	28
224	236	193	91	93	118	97	52	33	48	51	25	25	42	45	66
217	227	193	90	95	110	65	62	39	47	43	25	16	26	46	111
217	230	196	88	97	101	59	53	40	50	57	19	20	57	96	77
217	232	198	94	89	89	51	50	41	48	65	32	24	38	55	6
215	231	198	87	86	93	43	42	36	43	66	52	60	22	66	104
220	232	202	86	94	89	46	34	30	43	50	74	58	71	152	128
224	233	195	96	98	82	32	24	40	54	50	50	87	183	156	92
224	238	195	94	95	70	34	25	56	57	52	58	124	175	140	45
219	232	194	78	78	49	32	24	57	66	55	69	92	162	69	11
215	229	191	76	57	36	26	25	44	50	62	75	88	60	7	19
216	225	186	107	65	26	34	19	46	65	45	68	82	70	27	20
213	219	195	100	44	19	33	34	37	63	59	59	56	79	71	29
213	220	196	120	35	22	45	45	40	39	51	41	68	81	63	57
217	226	199	112	16	28	24	36	29	29	38	39	63	79	75	82
219	227	201	91	24	24	15	43	30	26	36	50	53	83	63	74
221	222	201	82	22	21	22	49	26	25	21	38	54	77	81	82
218	219	196	77	11	21	27	38	23	21	25	34	47	77	64	61
217	224	200	93	16	26	22	27	24	23	25	37	46	58	59	49
211	222	203	89	19	21	26	26	24	21	23	40	52	34	51	47
208	224	195	76	18	23	24	22	28	22	21	26	64	69	44	16
209	227	192	67	17	20	20	21	30	26	26	31	37	66	41	12

Kolom 17 – 32, Baris 26 – 35

21	29	24	20	91	197	210	157	92	84	78	71	127	197	235	239
25	22	23	34	158	210	179	76	36	36	125	100	120	177	244	167
18	20	14	105	201	182	135	146	120	120	191	185	131	169	236	160
18	13	63	183	186	114	168	200	198	182	186	187	160	169	232	215
12	25	137	193	80	129	180	206	228	224	220	203	180	168	227	229
36	67	198	91	40	138	176	200	217	228	221	196	170	159	216	230
38	130	134	11	59	132	171	192	202	208	210	176	156	153	204	234
106	165	31	18	77	128	167	187	195	202	201	170	141	133	179	219
120	64	12	30	86	133	165	185	190	202	202	191	170	177	204	201
71	20	31	34	81	134	169	181	188	187	189	188	192	227	233	183

Kolom 17 – 32, Baris 36 – 50

26	27	37	33	60	116	160	175	187	159	137	152	153	165	163	141
14	23	31	37	44	78	130	148	176	182	157	158	180	193	175	124
23	25	30	32	36	52	91	128	164	174	179	176	179	181	153	50
30	27	21	28	29	40	43	76	131	158	182	208	212	193	104	12
33	23	20	22	31	34	49	76	111	134	162	191	194	183	136	38
30	26	19	22	28	30	59	126	147	154	169	175	176	210	237	219
26	29	19	21	29	42	51	117	138	160	173	174	191	217	231	243
28	27	17	23	31	80	56	120	153	172	177	184	199	209	223	234
48	31	19	25	37	99	58	128	171	177	180	188	194	203	218	226
51	34	29	23	65	121	69	139	175	176	179	185	190	201	210	222
48	52	32	30	104	131	76	151	176	178	176	181	188	196	206	217
24	34	19	53	131	108	93	174	183	181	176	176	185	196	199	209
21	21	29	87	132	70	130	177	187	186	183	178	181	192	197	207
18	19	61	122	89	83	170	178	185	188	187	180	179	183	193	202
12	36	95	88	68	145	176	180	184	187	190	185	181	182	189	197

Kolom 33 – 50, Baris 26 – 50

71	10	30	48	35	56	142	166	155	148	141	139	138	122	170	254	254	253
21	13	33	51	41	56	161	165	152	151	143	135	131	119	183	255	253	254
11	27	36	58	46	58	167	155	148	149	147	134	125	107	181	255	255	253
17	28	36	65	49	64	164	149	144	139	139	129	118	102	193	255	253	255
5	20	37	65	52	75	146	104	111	116	124	122	111	107	223	255	254	254
142	38	22	59	47	82	136	112	100	92	89	90	85	99	235	255	253	214
255	214	79	33	39	85	151	140	124	114	95	79	93	110	238	255	217	79
247	255	239	72	19	98	157	140	138	126	111	98	113	173	255	255	133	46
243	252	255	194	20	103	155	143	134	129	115	105	166	238	255	222	84	74
237	255	255	255	79	100	153	141	131	120	106	129	245	255	255	166	76	94
232	245	252	255	147	105	147	131	121	119	104	157	253	255	232	123	87	96
224	241	255	255	221	123	120	128	129	122	115	154	213	255	197	95	82	72
220	234	250	255	255	114	57	78	91	99	137	155	181	253	147	69	66	71
213	231	246	253	255	142	59	59	40	23	84	203	233	219	64	47	65	71
209	224	239	249	255	189	74	82	63	31	78	240	215	92	31	57	67	53
146	62	58	26	58	77	25	25	15	75	148	176	168	166	162	159	154	152
35	74	31	16	56	90	25	20	25	109	163	171	160	164	160	159	150	143
103	108	43	21	54	95	25	21	43	133	170	166	157	161	157	153	140	125
164	111	70	25	50	101	26	16	70	149	169	160	157	152	148	141	121	134
187	152	91	25	45	108	23	24	108	165	163	153	153	146	142	124	135	220
181	153	77	24	40	113	28	40	136	171	159	153	149	141	133	126	206	254
175	139	43	26	36	110	38	67	153	169	157	152	146	136	121	165	249	251
169	104	19	35	33	105	59	104	164	157	148	147	144	136	128	212	255	250
156	59	8	38	31	88	91	145	165	155	147	146	141	129	145	240	254	252
124	24	18	47	33	70	118	158	163	151	143	143	141	125	157	250	254	255

Matriks $f(x,y)^{Green} =$

Kolom 1 – 16, Baris 1 – 25

74	68	42	19	22	22	20	23	34	37	40	44	40	42	43	38
72	68	43	17	18	22	21	25	34	37	37	39	39	39	42	42
69	68	42	13	16	23	22	24	31	36	37	39	37	37	41	39
69	69	42	11	14	22	21	24	31	34	36	36	37	36	36	35
72	68	41	7	11	18	18	24	29	32	33	32	36	35	46	47
73	67	37	3	8	16	15	19	27	28	31	32	33	39	38	40
73	69	37	4	11	17	14	18	26	29	33	30	35	31	30	37
75	70	37	4	13	18	15	16	26	30	31	34	28	29	31	37
73	70	36	5	12	16	14	14	24	28	33	31	27	28	31	34
70	70	35	5	10	14	16	16	24	27	39	22	24	25	31	39
71	68	35	3	7	12	14	16	23	29	61	16	22	27	34	44
74	70	35	4	7	12	11	16	23	48	70	14	27	30	35	37
75	75	38	6	11	19	12	14	20	69	57	16	22	27	33	33
79	81	40	2	8	19	15	14	20	83	58	16	21	24	30	35
81	81	42	2	6	17	14	14	17	90	67	30	19	25	33	51
80	77	43	3	6	12	8	10	12	87	72	38	17	27	44	46
82	80	44	2	6	13	9	7	13	108	87	51	28	40	41	43
83	80	44	2	8	15	12	10	8	107	109	39	36	33	38	46
81	79	45	2	6	12	11	11	3	80	122	52	41	33	40	38
80	79	45	2	6	11	8	9	7	44	129	86	41	39	34	36
82	81	46	2	4	7	6	7	18	11	98	119	40	34	39	40
82	84	46	2	5	7	7	7	20	15	82	114	26	32	35	27
82	84	45	1	6	9	7	7	23	21	49	81	20	35	20	4
83	85	47	4	6	9	8	10	22	23	27	38	35	31	9	7
83	88	48	4	5	10	8	6	17	33	39	23	35	11	11	15

Kolom 17 – 32, Baris 1 – 10

37	40	39	36	38	42	44	41	43	42	38	39	39	38	39	31
37	36	31	31	36	40	41	40	42	39	38	39	38	40	39	32
35	33	29	29	35	38	38	34	36	38	38	38	37	39	35	34
34	45	53	64	86	100	92	79	54	33	35	39	36	36	33	31
45	60	68	77	96	110	122	132	137	104	47	25	32	32	31	26
42	51	56	64	82	105	123	132	142	154	138	74	22	25	29	26
42	47	52	56	70	99	127	136	141	147	159	173	139	41	18	22
39	45	51	55	66	93	119	127	147	171	181	183	199	138	12	14
41	51	55	58	60	81	112	151	170	168	166	174	180	195	126	22
48	54	48	41	59	109	145	151	150	159	172	176	178	179	198	143

Kolom 17 – 32, Baris 11 – 25

47	47	40	58	110	128	125	136	154	158	166	173	175	178	188	207
39	38	69	99	104	114	122	140	138	146	154	162	171	175	176	189
37	64	80	87	103	114	119	113	121	134	147	158	149	147	169	172
56	60	66	83	99	100	99	107	112	117	130	129	130	143	148	141
53	59	69	72	87	93	96	103	104	99	108	120	131	130	121	114
48	56	60	69	77	87	88	88	87	88	93	103	106	100	99	107
49	48	56	62	59	54	64	70	69	74	76	69	69	88	117	144
42	45	49	48	40	26	31	58	31	21	12	8	57	124	154	151
40	45	40	27	21	9	18	25	22	8	12	57	112	135	141	138
38	29	18	7	6	7	14	14	25	23	71	129	131	119	119	130
31	12	11	4	13	6	3	6	25	62	115	132	117	112	119	128
10	3	7	9	16	17	1	16	53	104	128	106	104	101	126	143
4	2	2	3	17	19	14	72	102	106	127	93	80	104	138	148
6	7	2	4	9	19	59	95	129	106	89	77	86	106	133	142
4	3	2	11	10	48	105	109	121	58	36	43	77	93	113	128

Kolom 33 – 50, Baris 1 – 25

86	27	57	53	29	0	0	65	150	149	49	0	2	1	1	2	2	47
171	48	56	56	18	13	92	168	189	203	110	2	0	0	3	0	33	69
178	134	52	57	81	134	178	177	171	190	108	0	1	4	0	18	67	74
142	146	107	131	161	174	168	170	169	191	73	2	1	2	4	52	73	75
115	131	155	165	161	162	168	145	123	155	33	0	0	0	35	71	75	78
133	152	154	150	158	168	169	100	78	90	5	0	0	13	61	74	78	75
149	146	156	166	172	178	117	40	85	69	1	1	2	40	71	77	76	74
151	155	164	166	128	66	18	56	91	12	0	0	15	63	76	79	76	75
143	154	125	80	33	32	80	82	7	1	2	0	38	76	83	82	80	80
133	75	27	42	70	91	70	7	0	3	0	10	59	80	86	84	82	77
130	54	12	46	65	38	0	0	0	1	2	27	64	89	85	86	81	80
148	90	0	14	57	5	0	2	4	0	9	49	71	85	85	84	83	82
163	128	9	2	51	12	2	1	1	0	28	69	79	72	76	77	79	81
160	157	35	0	38	17	0	2	2	3	49	78	85	81	81	76	71	71
135	105	24	0	33	27	0	2	2	17	58	79	79	78	85	80	75	73
29	55	72	67	69	64	61	62	60	63	140	153	45	28	34	35	37	39
28	44	68	71	67	65	63	63	63	54	87	173	123	28	33	35	41	33
30	42	60	66	66	65	63	63	60	54	52	127	187	77	21	35	33	14
28	43	54	58	62	60	60	59	54	49	46	68	171	154	33	19	3	1
25	42	52	52	56	57	54	53	50	47	47	44	99	191	87	0	2	1
23	41	56	50	44	51	51	48	48	48	47	46	53	107	33	0	5	8
22	40	61	54	34	34	51	50	49	46	46	51	45	8	1	1	2	1
19	41	60	57	28	7	41	52	46	47	45	48	19	1	1	3	3	1
7	43	58	55	27	1	21	48	45	43	46	27	1	1	1	1	0	2
10	35	56	55	29	1	1	22	51	43	33	5	0	1	1	2	0	10

Kolom 1 – 16, Baris 26 – 50

84	88	48	3	4	12	6	7	38	55	47	23	11	14	17	11
86	88	49	3	8	9	3	15	88	59	19	7	9	17	22	2
86	94	52	5	14	18	19	37	76	38	17	15	9	25	37	5
88	97	57	6	14	24	50	41	7	3	36	19	10	35	41	8
84	90	54	8	13	35	43	23	7	26	28	3	7	21	21	24
82	85	51	5	20	36	29	23	12	31	25	0	2	2	11	44
82	85	52	9	30	36	23	22	21	39	37	1	2	12	28	29
82	88	57	14	15	19	19	25	22	29	48	7	3	14	15	1
78	90	58	7	8	25	12	20	14	26	54	32	12	4	33	47
80	93	59	5	19	22	21	9	4	14	27	49	18	33	92	51
85	94	58	19	23	23	10	4	19	31	21	31	30	109	81	32
88	95	65	21	25	21	13	6	39	44	27	35	47	74	54	15
87	93	59	7	19	12	12	2	41	54	42	36	41	76	18	0
84	91	54	5	12	11	5	1	27	30	49	52	37	21	1	1
80	85	56	36	22	6	2	1	33	42	24	57	60	42	17	2
75	83	67	27	15	5	7	13	15	43	43	42	39	51	46	7
77	83	62	47	7	2	19	20	10	20	29	20	51	60	37	27
85	87	65	45	0	7	3	10	4	10	15	13	41	62	47	48
85	89	62	25	6	4	1	23	10	8	11	25	28	62	48	49
86	93	65	24	2	2	6	28	6	1	2	18	33	61	63	63
83	91	67	23	0	3	7	10	2	2	6	12	32	61	46	37
79	88	66	26	1	6	4	3	3	3	5	13	30	46	37	29
78	88	64	22	1	3	5	5	4	2	5	21	33	19	27	26
76	88	65	17	2	1	4	2	2	2	1	8	49	49	20	0
77	94	66	19	1	1	1	3	4	5	6	5	17	47	20	1

Kolom 17 – 32, Baris 26 – 35

6	13	5	4	34	106	139	87	24	12	16	5	20	58	106	120
7	8	6	8	76	139	105	8	0	11	86	36	11	37	120	77
2	1	0	45	121	110	36	37	28	39	102	67	19	36	139	75
0	1	16	97	110	18	39	67	66	62	68	71	36	28	135	123
0	4	61	117	23	13	40	66	90	98	94	67	41	24	126	137
12	23	117	48	0	21	33	50	74	91	84	56	35	20	104	138
7	65	75	0	3	14	33	43	57	68	71	42	23	21	80	148
56	83	11	2	9	16	27	37	51	59	62	37	18	9	50	105
53	27	0	6	17	15	23	32	43	52	64	56	37	61	101	82
23	0	1	4	15	16	24	30	33	41	46	50	56	110	123	69

Kolom 17 – 32, Baris 36 – 50

7	1	2	3	7	12	24	26	38	27	15	16	21	40	36	30
0	3	1	3	2	7	16	24	36	38	22	9	24	49	47	28
2	4	2	0	2	2	6	23	30	35	41	42	48	50	44	7
1	1	3	0	3	1	2	8	19	33	50	69	79	67	22	1
3	1	1	2	1	3	3	14	23	33	42	60	65	71	60	17
1	2	1	0	4	1	4	26	34	37	42	44	51	96	139	135
2	2	1	1	3	0	8	25	28	37	39	38	62	95	119	132
9	1	3	2	3	6	7	25	32	38	37	45	63	80	100	112
23	1	3	1	1	8	9	28	32	34	38	45	55	70	90	108
23	0	3	1	7	17	10	29	35	36	36	41	53	68	79	101
19	13	4	0	12	20	12	32	38	39	33	38	47	60	73	92
2	6	4	2	13	15	17	35	39	37	33	36	43	55	68	82
1	0	0	8	19	7	28	37	41	40	35	35	42	50	63	76
2	0	3	14	8	15	35	35	37	40	39	32	34	44	58	68
2	2	7	7	7	29	36	37	37	39	40	35	33	40	52	63

Kolom 33 – 50, Baris 26 – 50

14	0	2	2	0	25	57	66	75	70	73	69	68	57	82	161	173	168
3	1	3	5	1	21	66	71	76	73	71	69	69	57	97	182	179	179
1	3	2	9	2	20	73	74	77	76	75	70	66	53	113	193	184	180
1	2	4	12	1	19	74	73	77	75	74	71	65	51	133	193	174	178
1	0	6	10	2	23	59	38	45	57	67	67	63	58	154	176	164	150
88	20	1	8	0	26	56	47	36	31	29	30	40	49	145	158	156	100
156	139	47	1	0	26	65	67	60	51	40	27	25	40	148	165	109	17
136	167	168	40	0	34	70	70	65	63	57	52	37	77	172	154	44	0
131	158	190	136	2	36	71	68	64	62	57	47	69	137	177	113	9	6
128	158	175	181	42	34	73	68	65	58	50	56	152	171	162	55	2	16
124	156	173	184	93	40	76	67	64	62	48	71	157	168	118	24	10	14
112	145	165	180	142	50	61	65	68	68	58	57	92	161	76	6	7	4
98	134	165	175	172	42	8	22	37	50	64	53	86	152	37	1	5	13
88	122	158	172	180	73	4	6	0	2	34	93	127	104	3	1	10	18
78	106	144	167	181	117	22	26	10	1	27	124	89	21	1	10	19	5
47	4	4	0	23	29	0	1	1	27	68	77	73	73	76	77	75	76
0	27	1	0	22	32	0	1	4	46	74	75	70	70	71	73	74	72
36	31	1	1	19	37	1	0	14	62	76	72	71	70	73	71	69	63
46	16	6	0	17	44	0	0	29	66	75	71	72	71	71	69	61	70
56	28	7	0	11	52	1	2	44	72	74	70	70	70	67	62	68	116
54	29	6	0	9	52	4	10	59	77	73	68	65	67	64	62	105	124
50	25	1	2	5	52	10	24	69	76	72	71	70	68	62	84	124	125
43	17	0	1	1	51	21	40	74	75	72	69	68	68	60	110	127	149
36	12	2	3	1	43	35	55	75	72	67	70	68	65	72	119	145	164
25	4	3	3	0	34	48	63	75	71	69	69	68	61	76	134	163	165

Matriks $f(x,y)^{Blue} =$

Kolom 1 – 16, Baris 1 – 25

0	2	3	3	4	4	0	1	0	6	4	2	2	2	0	4
0	3	4	2	3	3	2	2	4	3	1	1	1	1	3	3
2	3	2	1	3	4	0	1	1	1	1	4	1	0	2	0
3	1	3	2	3	3	0	2	3	3	1	1	5	2	0	3
3	1	3	4	3	2	1	5	3	5	2	1	3	1	10	13
3	1	3	3	3	3	2	2	4	0	2	2	0	8	4	4
1	2	4	3	3	4	3	3	2	2	2	1	7	5	1	2
1	2	3	3	4	4	3	2	2	4	2	3	2	2	4	0
1	4	2	4	3	3	5	4	4	2	1	3	3	0	1	4
0	2	2	4	3	2	6	3	3	1	7	6	1	1	2	3
0	3	2	2	2	2	5	1	0	4	15	2	3	4	5	1
1	5	4	2	1	3	4	3	2	11	17	3	4	0	3	1
0	3	4	5	4	6	2	2	3	21	7	4	2	6	6	3
1	4	0	3	2	2	0	3	2	23	7	1	4	0	4	4
1	4	1	1	1	2	3	4	6	22	5	4	2	5	6	7
2	5	4	2	3	5	4	2	7	15	6	7	2	3	5	6
2	1	1	3	3	3	2	1	7	32	5	6	5	3	6	5
4	1	2	3	4	5	5	3	4	31	16	3	5	3	5	4
2	0	3	3	2	3	4	4	2	29	21	3	8	3	7	0
1	0	1	3	2	2	4	5	0	18	34	12	7	6	8	7
3	2	2	3	1	2	2	3	0	1	33	21	6	2	5	15
2	4	3	3	4	3	3	2	5	0	33	35	1	2	7	3
1	2	2	2	3	5	4	2	5	2	15	29	0	5	4	5
2	3	2	2	3	5	3	2	4	0	5	14	19	9	7	7
3	0	5	3	2	0	5	2	0	4	11	15	19	7	13	16

Kolom 17 – 32, Baris 1 – 10

0	0	3	3	3	0	0	1	1	0	3	1	1	4	2	2
1	3	1	1	1	2	2	3	0	0	2	1	1	4	2	2
2	1	1	0	3	4	2	0	0	4	1	5	4	2	0	2
5	14	21	30	49	61	53	38	19	1	1	2	1	2	4	0
10	25	35	42	59	71	77	80	83	60	14	0	5	2	1	3
6	13	18	25	44	64	74	80	87	98	87	36	0	1	0	5
5	6	9	13	26	52	77	87	86	94	105	124	99	13	0	1
2	3	7	9	18	44	69	76	98	119	128	130	142	99	1	0
4	4	5	7	9	34	62	101	119	116	114	120	130	141	84	14
4	9	6	0	19	60	92	92	98	105	118	122	126	122	143	101

Kolom 17 – 32, Baris 11 – 25

5	3	5	23	59	77	71	78	99	102	116	122	119	122	133	156
5	3	28	50	54	60	72	83	88	93	107	112	113	121	125	139
7	14	21	36	50	64	71	65	69	82	97	104	94	95	115	119
9	11	14	31	51	49	45	54	61	65	81	78	79	93	100	99
5	12	19	22	42	44	42	48	53	51	64	72	82	86	79	75
6	8	13	21	25	39	45	37	35	34	43	56	61	63	60	64
6	8	12	19	24	31	40	42	36	34	40	37	41	46	64	85
4	3	7	14	20	16	32	57	36	19	11	8	29	68	100	98
5	6	5	11	22	9	23	28	22	12	11	27	59	77	89	84
5	7	5	6	9	5	13	12	30	20	37	80	77	74	67	80
16	8	9	6	14	6	6	9	28	58	67	83	71	68	74	81
2	3	9	9	17	17	0	8	36	71	77	64	63	52	74	85
5	2	4	2	22	25	3	32	61	70	80	42	23	44	74	85
7	9	1	4	13	16	22	36	79	68	41	18	26	47	71	80
5	5	3	12	9	21	48	58	72	26	2	12	27	27	50	65

Kolom 33 – 50, Baris 1 – 25

63	2	1	3	0	0	0	44	102	102	25	0	4	3	0	2	3	20
132	10	0	0	0	15	65	113	132	145	79	0	1	7	0	2	16	22
131	95	0	7	46	94	122	120	111	130	73	1	0	4	0	10	28	22
102	103	55	75	100	110	112	112	117	134	53	0	0	0	5	20	24	18
74	83	100	103	105	105	114	90	70	101	21	0	2	0	14	21	21	15
77	97	102	101	108	112	115	45	31	55	3	0	0	9	22	21	18	14
93	95	101	110	117	121	67	10	48	45	0	1	2	13	22	25	16	16
97	101	109	110	84	34	4	30	62	6	1	0	11	21	31	21	20	24
90	102	81	47	11	1	26	48	5	1	3	1	17	30	35	31	33	32
84	45	15	33	19	16	29	3	0	0	0	7	21	30	34	34	33	30
75	23	7	32	33	10	0	1	0	3	3	15	26	35	33	33	26	29
88	40	2	10	38	7	0	1	6	1	6	15	29	36	34	32	32	30
99	67	2	2	34	2	3	3	0	2	14	24	26	28	31	29	31	35
99	91	9	0	28	8	6	2	3	5	18	25	25	27	34	26	27	32
72	52	7	1	22	12	0	2	3	6	19	15	15	25	24	26	25	29
5	5	2	2	0	6	4	0	4	2	33	46	3	2	2	0	2	2
0	4	5	4	2	4	4	3	2	0	12	61	34	0	1	0	2	4
3	3	3	5	1	1	1	3	1	1	0	32	76	11	2	2	4	7
5	2	1	2	0	2	2	2	2	0	2	4	61	49	2	4	2	1
0	0	2	0	2	3	3	3	2	4	2	1	17	73	24	0	3	4
1	0	4	0	3	2	2	0	2	0	2	3	2	32	10	0	7	6
3	1	5	0	3	2	3	1	0	2	1	0	2	0	4	3	4	3
2	2	1	3	0	3	3	3	1	3	0	0	2	1	3	0	3	2
0	3	0	0	2	0	6	2	4	0	1	2	3	4	4	0	3	3
0	0	5	4	1	3	3	0	6	1	1	0	0	4	1	2	4	5

Kolom 1 – 16, Baris 26 – 50

3	1	1	4	1	3	3	7	13	4	8	12	12	17	22	13
4	2	1	0	5	3	2	9	37	12	3	5	11	23	25	0
1	0	5	2	6	3	10	21	46	26	19	22	12	31	41	4
0	0	5	0	3	6	26	30	9	5	45	26	6	41	47	7
5	4	0	4	2	17	43	27	8	29	34	5	7	28	21	10
1	3	3	2	15	23	29	24	17	42	25	3	2	2	9	18
1	4	2	4	24	30	25	27	25	47	39	1	2	6	15	15
1	2	4	7	6	7	22	31	24	35	56	10	0	12	15	0
0	2	0	0	4	14	17	23	17	34	58	33	2	0	24	30
1	2	1	1	14	14	24	12	7	18	37	55	16	22	58	33
2	1	6	13	17	17	12	5	26	39	26	33	23	74	49	22
2	3	13	15	17	16	12	8	49	51	33	41	37	44	19	7
2	2	4	3	15	6	11	4	44	68	52	43	37	43	1	1
2	2	0	1	7	7	4	1	37	39	59	60	33	16	1	0
2	0	6	30	16	7	3	0	40	48	29	65	62	39	16	2
2	7	20	18	7	5	6	8	17	52	44	48	45	48	41	9
0	3	9	28	6	4	22	23	10	22	32	25	59	65	36	19
0	6	12	26	1	4	2	13	8	12	21	16	44	68	46	36
0	1	3	11	6	5	1	25	12	6	15	28	31	67	45	44
4	2	3	13	4	4	7	27	5	1	4	20	38	64	61	59
2	4	9	13	1	1	6	7	1	4	8	15	37	64	42	35
4	2	3	9	4	7	4	3	0	5	4	13	33	48	39	28
1	3	5	6	1	1	4	4	5	4	5	23	35	16	27	25
1	2	3	9	5	3	6	3	3	3	2	8	54	50	16	0
3	3	7	7	1	3	3	3	3	4	7	6	18	49	19	0

Kolom 17 – 32, Baris 26 – 35

1	13	7	4	15	49	83	53	11	0	5	6	2	3	40	64
7	8	12	7	38	83	68	5	0	14	69	24	4	1	58	40
3	3	0	19	68	72	7	0	5	18	70	31	0	3	86	36
0	3	8	48	74	6	0	11	17	12	28	24	2	1	93	72
2	3	25	68	16	0	5	7	27	37	35	15	0	0	84	86
2	10	72	29	0	4	1	0	6	23	16	5	3	0	67	87
4	27	45	0	4	2	5	1	4	6	6	4	4	0	44	97
29	46	2	2	6	2	2	2	1	3	3	2	3	1	19	51
26	19	0	6	10	3	1	1	0	2	2	1	2	24	60	26
19	2	3	2	3	6	3	3	2	0	2	1	4	56	70	19

Kolom 17 – 32, Baris 36 – 50

3	0	0	3	3	3	2	2	5	4	2	4	8	22	17	2
0	5	3	4	4	1	6	0	3	3	2	2	11	22	12	4
1	3	1	1	1	3	3	1	3	2	4	4	4	8	1	1
3	2	1	1	4	6	0	5	5	1	2	12	20	17	0	0
1	3	3	1	1	1	3	3	1	5	5	8	10	21	34	14
3	0	0	3	2	5	0	2	4	2	1	2	3	36	78	73
2	7	0	0	4	2	2	4	3	3	2	0	4	28	55	60
5	4	3	1	0	3	0	5	3	3	1	2	3	14	33	37
19	0	3	1	3	5	4	5	1	2	2	1	0	5	19	34
22	1	4	3	6	4	2	2	2	3	4	6	1	3	9	32
15	14	3	0	1	1	3	2	1	0	1	4	2	0	6	28
5	5	1	1	3	7	3	2	2	0	1	1	3	2	0	15
0	0	4	3	3	2	5	2	2	1	5	1	1	4	2	8
2	2	2	4	4	2	3	1	1	2	3	2	3	1	2	5
1	1	5	3	2	4	3	3	3	1	3	2	3	2	0	2

Kolom 33 – 50, Baris 26 – 50

3	3	1	4	1	20	16	6	14	21	26	20	17	15	8	42	66	62
1	3	5	5	1	17	18	7	24	25	21	21	18	16	22	67	74	78
0	3	3	4	1	11	21	18	25	25	25	32	22	15	42	84	80	77
2	3	5	4	1	13	24	21	25	27	32	33	25	20	60	82	69	70
0	0	4	3	1	12	14	3	11	15	24	28	27	25	61	55	50	37
52	16	0	4	1	9	7	5	1	2	3	6	11	16	33	35	43	12
76	82	26	2	2	10	14	14	12	10	9	6	2	6	38	53	21	2
57	91	104	29	0	9	16	19	12	20	19	18	1	16	54	40	2	3
55	84	124	86	2	7	9	11	13	17	17	10	1	29	56	18	3	3
59	97	112	116	24	0	14	17	15	19	13	13	48	47	46	2	3	3
59	90	106	118	55	8	30	21	21	19	13	12	34	52	22	1	4	3
49	84	102	118	85	9	21	22	24	22	15	2	9	43	7	2	4	3
33	74	101	112	108	17	1	5	11	17	13	4	18	34	2	2	4	2
21	55	95	109	113	42	1	0	0	1	7	4	18	15	2	3	3	4
8	36	86	107	118	67	1	3	2	1	6	13	4	1	3	2	5	3
15	0	4	0	17	17	0	1	1	13	17	10	5	12	15	17	19	27
4	19	0	1	12	20	2	3	3	13	14	14	7	9	11	14	24	28
17	23	5	2	13	23	0	1	8	18	14	10	12	15	11	21	23	22
8	0	4	0	12	25	3	1	9	16	11	11	15	16	19	21	24	24
4	2	5	3	9	29	3	4	8	11	14	16	16	18	25	23	23	19
0	3	2	0	7	31	4	0	7	13	12	13	18	20	22	26	13	0
2	0	2	2	3	32	7	5	7	9	8	16	18	21	22	21	4	5
2	0	1	2	2	27	12	4	11	15	14	20	16	21	21	12	0	33
2	6	2	1	1	24	12	3	12	18	16	20	13	19	21	2	24	56
2	3	0	2	0	18	12	9	11	18	20	24	17	15	10	11	49	53

BIODATA PENULIS

Penulis dilahirkan di Gresik, pada 26 Maret 1991, merupakan anak ketiga dari tiga bersaudara. Penulis telah menempuh pendidikan formal yaitu di SD NU 1 Trate Gresik, SMP Negeri 1 Gresik dan SMA Negeri 1 Gresik. Setelah lulus dari SMA tahun 2009, penulis melanjutkan ke ITS melalui jalur PMDK Reguler dan diterima di Jurusan Matematika FMIPA ITS dengan NRP 1209 100 033. Di jurusan Matematika ini Penulis mengambil Bidang Ilmu Komputer. Selama menempuh perkuliahan penulis aktif dalam beberapa organisasi diantaranya Badan Eksekutif Mahasiswa (BEM ITS) dalam kementerian Pengembangan Sumber Daya Mahasiswa (PSDM), Himpunan Mahasiswa Matematika (HIMATIKA ITS) dalam departemen Pengembangan Sumber Daya Mahasiswa (PSDM) dan Lembaga Dakwah Jurusan Ibnu Muqlah (IM) dalam bidang kaderisasi. Penulis juga aktif di beberapa kegiatan yang diselenggarakan oleh Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, dan Institut Teknologi Sepuluh Nopember (ITS) Surabaya.

Informasi yang berhubungan dengan Tugas Akhir ini dapat ditujukan ke alamat email ievarrezt.trilly@gmail.com.